Payment Card Industry (PCI)

Technical Report

for

PCI Demo

Customer Contact	**ASV Contact**
Demo Report PCI Demo 138 Middle Street, Nieuw Muckleneuk 0181, South Africa Phone: 27 12 460 0880, Fax: 27 12 460 0885 support@sensepost.com	PCI Services SensePost (Pty) Ltd P.O. Box 176, Groenkloof, 0027, Republic of South Africa +27 (0)12 460-0880 pci@sensepost.com

Table of Contents

Vulnerability Level Overview

The following tables describe the vulnerability impact levels and vulnerability categories used in this document.

Vulnerability Impact Levels

Level 5 	**Urgent**	Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, and remote execution of commands as a root or administrator user.The presense of backdoors and Trojans qualify as Level 5 vulnerabilities.
Level 4 	**Critical**	Level 4 vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information qualify as Level 4 vulnerabilities
Level 3 	**High**	Level 3 vulnerabilities provide hackers with access to specified information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contenst, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to DoS attacks and unauthorised use of services such as mail relaying.
Level 2 	**Medium**	Level 2 vulnerabilities expose some sensitive information from the host, such as precision version of services. With this information, hackers could research potential attacks against a host.
Level 1 	**Low**	Level 1 vulnerabilities expose information such as open ports

Vulnerability Categories

Vulnerabilities	Vulnerabilities which have been determined to exist.
Potential Vulnerabilities	Vulnerabilities which appear to exist, but which have not been verified.
Vulnerabilities with compensating controls	Vulnerabilities which exist, but for which there exist compensating controls.
False Positive	This issue was reported by the scanner, but was determined to be a false-positive by manual verification.

Scan Details

SensePost (Pty) Ltd. has determined that PCI Demo is not compliant with the PCI scan validation requirement.

This report was generated by a PCI Approved Scanning Vendor, SensePost (Pty) Ltd., under certificate number 4239-01-01, within the guidelines of the PCI data security initiative.

Scan Overview

Scan Created: 2009-12-04 09:30:34

Scan Initiated: 2009-12-07 16:38:02

Scan Completed: 2009-12-07 17:22:36

Report Date: 2010-03-26 16:32:56

Responsible Agent: localhost

Comments regarding the scan:

As per the PCI policy, the customer has confirmed that any IDS or IPS systems which they use have been configured not to block the IP addresses or hosts used for scanning by the vendor.

Target List

IP Address	192.168.235.49
IP Address	192.168.235.50
IP Address	192.168.235.51
IP Address	192.168.235.52
IP Address	192.168.235.54
IP Address	192.168.235.55
IP Address	192.168.235.56
IP Address	192.168.235.57
IP Address	192.168.235.58
IP Address	192.168.235.59
IP Address	192.168.235.60
IP Address	192.168.235.61

PCI Status

Overall PCI Status

[FAILED]

According to the PCI Standard, to be considered compliant, a component must not contain vulnerabilities assigned Level 3, 4 or 5. To be considered compliant, all components within the customer infrastructure must be compliant.

PCI Status per Host Scanned

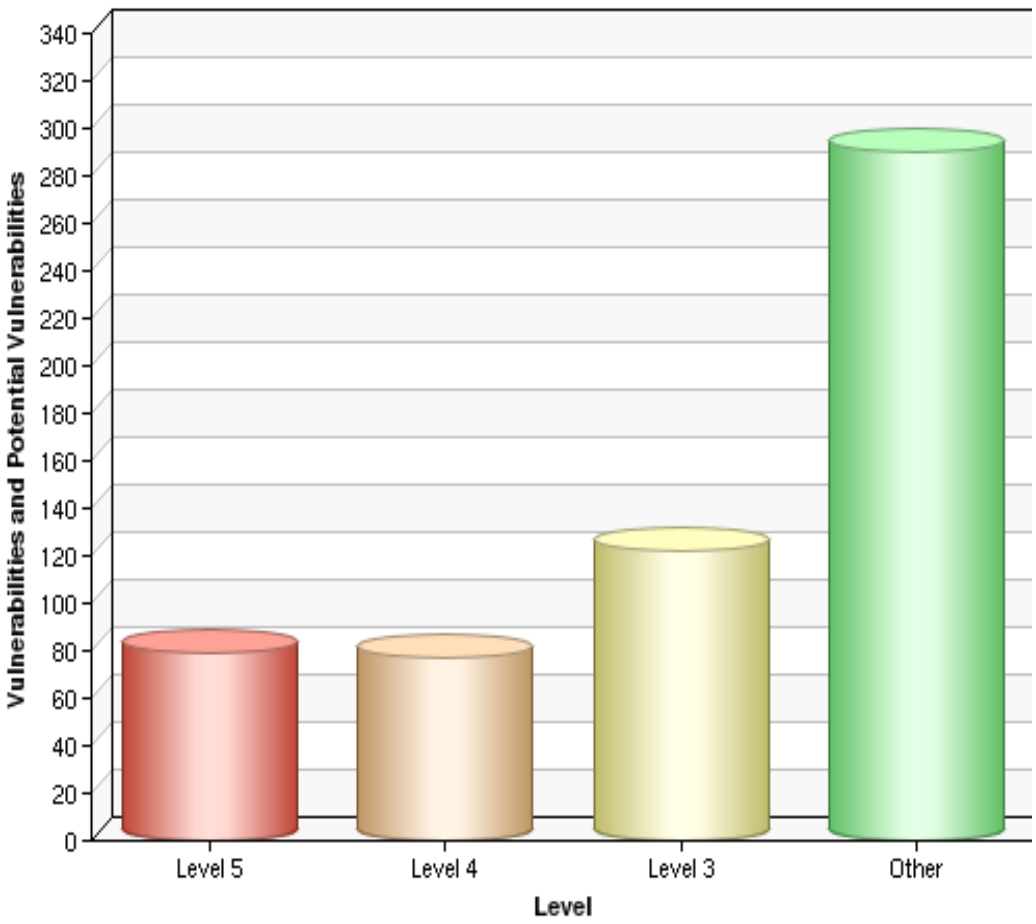
Target	Risk Rating	PCI Status
192.168.235.49	98	[FAILED]
192.168.235.50	0	[COMPLIANT]
192.168.235.51	73	[FAILED]
192.168.235.52	36	[FAILED]
192.168.235.54	86	[FAILED]
192.168.235.55	28	[FAILED]
192.168.235.56	114	[FAILED]
192.168.235.57	24	[FAILED]
192.168.235.58	41	[FAILED]
192.168.235.59	161	[FAILED]
192.168.235.60	133	[FAILED]
192.168.235.61	72	[FAILED]

Summary of Vulnerabilities

Summary of Vulnerabilities

Impact Level	Vulnerabilities	Potential	Vulns. w. Controls	False Positives
Level 5 - Urgent	22	57	0	0
Level 4 - Critical	26	51	0	0
Level 3 - High	65	57	0	0
Level 2 - Medium	57	18	0	0
Level 1 - Low	215	0	0	0
Totals:	385	183	0	0

Compliance Issues by Level



192.168.235.49 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
Cisco IOS 12
PORT - Port/Protocol/Service/Banner Information
22/tcp(ssh) SSH-1.5-Cisco-1.25
PORT - Port/Protocol/Service/Banner Information
23/tcp(telnet)

Open Ports

Port	Protocol	Service	Comment
22	tcp	ssh	Banner - SSH-1.5-Cisco-1.25
23	tcp	telnet	Banner - User Access Verification
67	udp	bootps	Service - bootps
123	udp	ntp	Service - NTP
161	udp	snmp	Service SNMP

192.168.235.49 : Vulnerabilities

SNMP Weak / Guessable Community String

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-2001-0514, CVE-2002-0109, CVE-2004-0311, CVE-2004-1473, CVE-2004-1474

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10264
Bugtraq ID: 11237, 2112, 9681, 6825, 177, 10576, 7081, 7212, 7317, 986
CERT VU: 329230
CVE ID: 1999-0517, 2004-0311, 1999-0254, 1999-0516, 1999-0186, 2004-1473
Generic Exploit URL: http://packetstormsecurity.nl/0402-exploits/apc_9606_backdoor.txt
Generic Informational URL: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Guessable_Read_Community.html&fact_color=doc&tag=
Generic Informational URL: http://www.securiteam.com/exploits/Patrol_s_SNMP_Agent_3_2_can_lead_to_root_compromise.html
Generic Informational URL: http://www.securiteam.com/exploits/Windows_NT_s_SNMP_service_vulnerability.html
ISS X-Force ID: 1240, 15238, 1387, 1241, 1385, 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0460.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0517.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0527.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Microsoft Knowledge Base Article: 99880
Other Advisory URL: http://cert.uni-stuttgart.de/archive/bugtraq/1998/11/msg00249.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/advise12
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 10905, 12635
Security Tracker: 1011388, 1011389
Snort Signature ID: 1411, 1412, 1413, 1414, 1892, 1893, 2406
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-22-00178-1&searchclause=00178
Vendor Specific Advisory URL: http://www.auscert.org.au/render.html?it=494
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1582
Vendor Specific Solution URL: http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch
Vendor Specific Solution URL: http://www.sun.com/solstice/products/ent.agents/

192.168.235.49 : Vulnerabilities

Vendor URL: http://www.apcc.com/
Vendor URL: http://www.managementsoftware.hp.com/
Vendor URL: http://www.symantec.com/

Issue Description:

The SNMP community string on the remote host is still set to the default or can easily be guessed.

Simple Network Management Protocol (SNMP) is used to remotely manage or monitor a host or network device. If an attacker is able to guess the read community string, an attacker will be able to freely view information like the operating system version, IP addresses, interfaces, processes/services, usernames, shares, etc. If the write community string is guessable an attacker has the ability to change system information, leading to anything from a partial to full compromise of the remote host.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community
strings :
- public

Suggestions:

SNMP should preferably be removed if not in use.;;
Alternatively, the following security precautions should be put in place:;
- All community strings should be set to stronger, less easily guessable alternatives.;
- If SNMP is only used for monitoring purposes, write access should be disabled.;
- SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).;
- Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;;
For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:;
Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;

Writeable SNMP Information

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0792, CVE-2000-0147, CVE-2001-0380, CVE-2001-1210, CVE-2002-0478, CVE-2000-0515

Port/Protocol: 161/UDP

Other References:

192.168.235.49 : Vulnerabilities

Nessus NASL ID : 95160
Bugtraq ID: 973, 1327, 3758, 4330

Issue Description:

Unauthorized users can modify all SNMP information because the access password is not secure.

The system can be attacked in a number of ways--by route redirection, denial of service, complete loss of network service, reboots or crashes, and traffic monitoring.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community
strings :
- private

Suggestions:

If SNMP access is not required on this system, then disallow it. Otherwise, use a secure un-guessable "community name", and restrict the hosts that talk SNMP with your system to a defined list of IP addresses.

Cisco Default Password

Impact: Level 5 - Urgent

CVSS Score: 4.6

CVE Reference: CAN-1999-0508

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 23938

Issue Description:

The remote Cisco router has a default password set.
This allows an attacker to get a lot information about the network, and possibly to shut it down if the 'enable' password is not set either or is also a default password.

Raw Scanner Output:

Plugin Output :
It was possible to log in as 'cisco'/'cisco'

192.168.235.49 : Vulnerabilities

Suggestions:

Access this device and set a password using 'enable secret'

SSH Weak Cipher Used

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95192

Issue Description:

SSH is used to secure communication between a user and a server.

If weak ciphers are used by SSH to protect the session data, it is possible for a third party to record the network traffic, mount an offline bruteforcing attack, recover the session key and from there recover the content of the whole SSH session. It is perhaps also possible to recover usernames, passwords and other sensitive information.

Raw Scanner Output:

Cipher: des
Name Key Length(Bits): 64

Suggestions:

Where possible SSH should be configured not to use weak ciphers such as DES. A more secure alternative is available in most cases e.g. 3DES, AES.

Outdated SSH Protocol Versions Supported

Impact: Level 4 - Critical

CVE Reference: CVE-2001-0361, CVE-2001-1473 , CVE-2001-0572

Port/Protocol: 22/TCP

Other References:

192.168.235.49 : Vulnerabilities

Nessus NASL ID : 10882
Bugtraq ID: 2344
CERT VU: 61576, 997481, 888801, 161576
CIAC Advisory: I-047, m-017
CVE ID: 2001-0361, 2001-0572
Generic Informational URL: http://www.securityfocus.com/archive/1/161150
ISS X-Force ID: 6082
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2001-03/0225.html
Related OSVDB ID: 729
Snort Signature ID: 1324, 1325, 1326, 1327
Vendor Specific Advisory URL:
http://www.cisco.com/en/US/tech/tk583/tk617/technologies_security_advisory09186a00800b168e.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
Vendor Specific Advisory URL: http://www.debian.org/security/2001/dsa-027

Issue Description:

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Suggestions:

If you use OpenSSH, set the option 'Protocol' to '2'.
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.

UDP Constant IP Identification Field Fingerprinting Vulnerability

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2002-0510

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 95152
Bugtraq ID: 4314

Issue Description:

The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.
Normally, the IP Identification field is intended to be a reasonably unique value, and is used to

reconstruct fragmented packets. It has been reported
that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

Suggestions:

We are not currently aware of any fixes for this issue.

Management Interfaces Accessible On Cisco Device Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95191

Issue Description:

The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management.
These services can be accessed publicly, and are an invitation for malicious users to break in.
The port string mentioned with this vulnerability should identify the service in question.

Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

Raw Scanner Output:

Detected service snmp and os CISCO IOS VERSION 12.2(4)YB

Suggestions:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an
external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

192.168.235.49 : Vulnerabilities

Unencrypted Telnet Server

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 42263

Issue Description:

The remote Telnet server transmits traffic in cleartext.

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Suggestions:

Disable this service and use SSH instead.

Comments:

Created On: 2009-12-22 12:50:16
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across open networks such as the Internet.

Management Interfaces Accessible On Cisco Device Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 95191

192.168.235.49 : Vulnerabilities

Issue Description:

The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management.
These services can be accessed publicly, and are an invitation for malicious users to break in.
The port string mentioned with this vulnerability should identify the service in question.

Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and Denial Of Service are also possible.

Raw Scanner Output:

Detected service telnet and os CISCO IOS VERSION 12.2(4)YB

Suggestions:

Disable services that are not needed.
Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an
external firewall.
Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible.
Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.

Telnet Service and Version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 10281

Issue Description:

This detects the Telnet server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and types should be omitted where possible.

Raw Scanner Output:

Plugin output :
Here is the banner from the remote Telnet server :

192.168.235.49 : Vulnerabilities

```
---------------------------- snip ----------------------------
User Access Verification
Password:
---------------------------- snip ----------------------------
```

Suggestions:

Informational plugin.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

192.168.235.49 : Vulnerabilities

SSH Protocol Versions Supported.

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Synopsis :
A SSH server is running on the remote host.
Description :
This plugin determines the versions of the SSH protocol supported by
the remote SSH daemon.
Solution :
n/a
Risk factor :
None
Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
- 1.33
- 1.5
- 1.99
SSHv1 host key fingerprint :
8b:41:bf:ae:75:5a:0a:ab:2d:19:b2:d0:7a:36:b4:85

Suggestions:

Informational plugin.

NTP read variables

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.49 : Vulnerabilities

Port/Protocol: 123/UDP

Other References:

Nessus NASL ID : 10884

Issue Description:

A NTP (Network Time Protocol) server is listening on this port.

Theoretically one could work out the NTP peer relationships and track back network settings from this.

Raw Scanner Output:

Plugin output :
It was possible to gather the following information from the remote NTP
host :
system='cisco', leap=0, stratum=3, rootdelay=13.82,
rootdispersion=23.45, peer=11135, refid=132.246.168.148,
reftime=0xCEC8522E.47608CE3, poll=10, clock=0xCEC85511.22E71CFF,
phase=0.458, freq=73.91, error=0.78

Suggestions:

Quickfix: Set NTP to restrict default access to ignore all info packets:
restrict default ignore

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet:
RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall
protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets
with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN

192.168.235.49 : Vulnerabilities

flag.

Suggestions:

Many operating systems are known to have this behavior.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The remote clock is synchronized with the local clock.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.49 : Vulnerabilities

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.49 :
69.164.210.215
207.192.75.2
209.123.10.29
209.123.10.26
209.123.10.78
213.200.73.121
89.149.184.194
4.68.110.77
4.68.16.190
4.69.134.121
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.49 : Vulnerabilities

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A telnet server is running on this port.

Suggestions:

Informational plugin.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-1.5-Cisco-1.25

Suggestions:

192.168.235.49 : Vulnerabilities

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

192.168.235.49 : Vulnerabilities

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : CISCO IOS 12
CISCO PIX
Confidence Level : 69
Method : SSH
The remote host is running one of these operating systems :
CISCO IOS 12
CISCO PIX

Suggestions:

Informational plugin.

192.168.235.49 : Potential Vulnerabilities

Cisco Multiple Devices Crafted IP Option Multiple Remote Code Execution

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-0480

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 24741
Bugtraq ID: 22211
CERT VU: 341288
CVE ID: 2007-0480
FrSIRT Advisory: ADV-2007-0329
ISS X-Force ID: 31725
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-01/0554.html
News Article: http://www.theregister.co.uk/2007/01/25/cisco_ios_bug_fix/
Related OSVDB ID: 32091, 32093
Secunia Advisory ID: 23867
Security Tracker: 1017555
Vendor Specific Advisory URL:
http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb157.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

Issue Description:

The remote version of IOS contains a flaw which may cause the remote router to crash when processing specially malformed IP packets.

An attacker might use these flaws to execute arbitrary code on the remote routers.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb157.shtml

Cisco IOS System Timers Remote Overflow (CSCei61732)

Impact: Level 5 - Urgent

192.168.235.49 : Potential Vulnerabilities

CVSS Score: 9.3

CVE Reference: CVE-2005-3481

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 20134
Bugtraq ID: 15275
CVE ID: 2005-3481
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-11/0064.html
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml
Secunia Advisory ID: 17413
Security Tracker: 1015139

Issue Description:

The remote host is a CISCO router containing a version of IOS which is vulnerable to a heap overflow vulnerability.

An attacker may exploit this flaw to crash the remote device or to execute arbitrary code remotely.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

Cisco IOS SAA Malformed RTR Packet DoS (CSCdx17916, CSCdx61997

Impact: Level 4 - Critical

CVSS Score: 5

CVE Reference: CVE-2003-0305

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 11632
Bugtraq ID: 7607
CVE ID: 2003-0305
ISS X-Force ID: 12014
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml

192.168.235.49 : Potential Vulnerabilities

Issue Description:

It is possible to crash the remote router by sending malformed Response Time Responder (RTR) packets. For this flaw to be exploitable, the router needs to have RTR responder enabled. This bug is referenced as CISCO bug id CSCdx17916 and CSCdx61997

The RTR feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. With this feature you can perform troubleshooting, problem notifications, and problem analysis based on response time reporter statistics. A router is vulnerable only if the RTR responder is enabled.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml

Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-ud)

Impact: Level 4 - Critical

CVSS Score: 0

CVE Reference: CVE-2009-0631

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95157
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml

Issue Description:

Cisco IOS Software is affected by a denial of service vulnerability when multiple features of Cisco IOS software are enabled.
The vulnerability is caused due to an error in the way that Cisco IOS handles UDP packets, which can be exploited to block an interface of an
affected device by sending a specially crafted UDP packets. (CVE-2009-0631)
Devices running Cisco IOS and Cisco IOS XE with any of the following features are affected:
IP Service Level Agreements (SLA) Responder
Session Initiation Protocol (SIP)
Media Gateway Control Protocol (MGCP)

Successful exploitation of this vulnerability allows attackers to block an interface on the device, silently dropping any received traffic, which results in denial of service.

192.168.235.49 : Potential Vulnerabilities

Suggestions:

Workarounds:
1) Disable affected listening ports. Once disabled, confirm that the listening UDP port has been closed by entering the CLI command "show udp" or "show ip socket".
Impact of workaround #1: When applying this workaround to devices that are processing MGCP or H.323 calls, the device will not allow stopping SIP processing while active calls are being processed.
2) Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks.
3) Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device.
Impact of workaround #2 and #3: Because the features in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address,
which may defeat ACLs that permit communication to these ports from trusted IP addresses.
4) Use Cisco IOS Embedded Event Manager (EEM) policy to detect blocked interface queues. EEM can alert administrators of blocked interfaces with email, a syslog message, or a Simple Network Management Protocol (SNMP) trap.
Further information and examples on mitigating the vulnerability through workarounds can be found at the advisory cisco-sa-20090325-udp.
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-udp for additional information on obtaining the fixes.

Cisco IOS SSL Packets Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2007-2813

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95161
Bugtraq ID: 24097
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

Issue Description:

Multiple vulnerabilities exist in the implementation of SSL packets which lie in the processing of ClientHello, ChangeCipherSpec and Finished messages.
In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful exploitation of these vulnerabilities may lead to a sustained denial of service.

192.168.235.49 : Potential Vulnerabilities

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20070522-SSL for further information.

Cisco IOS Next Hop Resolution Protocol Vulnerability

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95193
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Issue Description:

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

Successful exploitation of the vulnerability may result in a restart of the device or remote code execution. Repeated exploitation may result in an extended denial of service condition.

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20070808 for further information.

Cisco IOS TCP Listener Crafted Packets Remote DoS

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2007-0479

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 24744

192.168.235.49 : Potential Vulnerabilities

Bugtraq ID: 22208
CERT VU: 217912
CVE ID: 2007-0479
FrSIRT Advisory: ADV-2007-0329
ISS X-Force ID: 31716
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-01/0552.html
News Article: http://www.theregister.co.uk/2007/01/25/cisco_ios_bug_fix/
Related OSVDB ID: 32091, 32092
Secunia Advisory ID: 23867
Security Tracker: 1017551
Vendor Specific Advisory URL:
http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb0e4.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

Issue Description:

The remote CISCO switch runs a version of IOS contains a flaw which may cause the remote router to crash when processing specially malformed TCP packets.

An attacker might use these flaws to crash this router remotely.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

Cisco IOS Multiple DLSw Denial of Service Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: No CVE Reference At This Time

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95155
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml

Issue Description:

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Malicious people can exploit these vulnerabilities to cause denial of service conditions.

192.168.235.49 : Potential Vulnerabilities

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080326-dlsw for information.

Cisco Telnet Denial of Service Vulnerability

Impact: Level 4 - Critical

CVSS Score: 10

CVE Reference: No CVE Reference At This Time

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 15627

Issue Description:

The remote router contains a version of IOS which has flaw in the telnet service which might allow an attacker to disable the administation of the remote router by SSH, HTTP and telnet.
An attacker may use this flaw to render this router un-manageable

Exploitation of this vulnerability may result in the denial of new telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation and HTTP connections to a device running IOS. Other access to the device via the console or SNMP is not affected. The device will remain in this state until the problematic TCP connection is cleared, or the device is reloaded (which will clear the problematic session). If no other access methods are available, exploitation of this vulnerability could deny remote access to the device.

Suggestions:

Solution : http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml
The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed. These worarounds are:
- Enabling SSH and disabling telnet
- Configuring a VTY Access Class
- Configuring Access Lists (ACLs)
- Configuring Infrastructure Access Lists (iACLs)
- Configuring Receive Access Lists (rACLs)
- Clearing Hung TCP Connections Using the IOS CLI
- Clearing Hung TCP Connections Using SNMP

192.168.235.49 : Potential Vulnerabilities

Cisco IOS ICMP Redirect Routing Table Modification

Impact: Level 4 - Critical

CVE Reference: CAN-2002-1222

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 11379
BugTraq: 6823

Issue Description:

It has been reported that it is possible to make arbitrary remote modifications to the Cisco IOS routing table.

If IP routing is disabled on a vulnerable router, the router will accept malicious ICMP redirect packets and modify its routing table accordingly. ICMP redirect messages are normally sent to indicate inefficient routing, a new route or a routing change. An attacker may specify a default gateway on the local network that does not exist, thus denying service to the affected router for traffic destined to any location outside the local subnet.

Suggestions:

Workaround:
The following workaround was suggested. It is possible to prevent the router from acting upon ICMP redirect packets by issuing the following command on the affected device:
Router(config)#no ip icmp redirect
Solution:
Users are advised to upgrade to the following IOS versions:
12.2(13.03)B
12.2(12.05)T
12.2(12.05)S
12.2(12.05)
12.2(12.02)S
12.2(12.02)T

Cisco IOS EIGRP Announcement ARP Denial of Service Vulnerability

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2002-2208

192.168.235.49 : Potential Vulnerabilities

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95164
Bugtraq ID: 6443
Vendor Reference: http://www.cisco.com/en/US/tech/tk365/technologies_security_notice09186a008011c5e1.html

Issue Description:

Internet Operating System (IOS) is the firmware developed and maintained by Cisco for Cisco routers.
A problem in IOS may make it possible for users to deny service to legitimate users of network resources.
A vulnerability has been reported in the handling of Enhanced Interior Gateway Routing Protocol (EIGRP),
Cisco's proprietary version of IGRP. EIGRP works by routers announcing their prescence via multicast.
When router discovery occurs, routers exchange network information via unicast transfer.
A system sending spoofed EIGRP announcements may cause a denial of service to all routers and systems on
a given network segment. Due to improper limits in the attempt to discover routers, a neighbor
announcement received by routers on a given network segment will result in an address resolution protocol
(ARP) storm, filling network capacity while routers attempt to contact the announcing neighbor.
Additionally, resources on the router such as CPU will also become bound while the router attempts to
reach the announcing neighbor. It should be noted that it is also possible to exploit this vulnerability
on systems that accept EIGRP announcements via unicast.

This vulnerability can make it possible for an attacker on a network to deny service to the local network
segment, as well as bordering network segments.

Suggestions:

The workaround for this issue is to apply MD5 authentication that will permit the receipt of EIGRP
packets only from authorized hosts. You can find an example of how to configure MD5 authentication for
EIGRP here.
If you are using EIGRP in the unicast mode then you can mitigate this issue by placing appropriate ACL
which will block all EIGRP packets from illegitimate hosts.

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip)

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2009-0636

Port/Protocol: 161/UDP

192.168.235.49 : Potential Vulnerabilities

Other References:

Nessus NASL ID : 95158
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml

Issue Description:

SIP (Session Initiation Protocol) is a signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination.
A denial of service vulnerability exists in the SIP implementation in Cisco IOS Software. This vulnerability is triggered by processing a specific and
valid SIP message. A remote attacker can exploit this vulnerability to cause the device to crash. (CVE-2009-0636) Cisco IOS devices with SIP voice services enabled are affected.

Successful exploitation of this vulnerability will result in a reload of the device. The issue could be repeatedly exploited to cause an extended denial of service condition.

Suggestions:

1) For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. On
some Cisco IOS software versions, SIP can be disabled using the following commands:
sip-ua
no transport udp
no transport tcp
Impact of the workaround: When applying this workaround to devices that are processing Media Gateway Control Protocol (MGCP) or H.323 calls,
the device will not stop SIP processing while active calls are being processed.
2) For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources.
Impact of the workaround: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may
defeat access control lists that permit communication to these ports from trusted IP addresses.
Further information and examples on disabling SIP and configuring CoPP to block SIP traffic can be found at the advisory cisco-sa-20090325-sip.
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-sip for
additional information on obtaining the fixes.

Cisco IOS Software Multiple Multicast Vulnerabilities (cisco-sa-20080924-multicast)

Impact: Level 4 - Critical

192.168.235.49 : Potential Vulnerabilities

CVSS Score: 7.8

CVE Reference: CVE-2008-3808, CVE-2008-3809

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95156
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml

Issue Description:

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS Software.
Devices that run Cisco IOS Software and are configured for PIM are affected by these issues.

Successful exploitation may cause a reload of the affected device. Repeated exploitation could result in a sustained denial of service condition.

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080924-ubr for more information.

Cisco IOS Interface DoS

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2003-0567

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 11791
Bugtraq ID: 8211
CERT VU: 411332
CERT: CA-2003-15, CA-2003-17
CVE ID: 2003-0567
ISS X-Force ID: 12631
Other Advisory URL: http://archives.neohapsis.com/archives/vulnwatch/2003-q3/0035.html
Secunia Advisory ID: 9288
Snort Signature ID: 2186, 2187, 2188, 2189
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

192.168.235.49 : Potential Vulnerabilities

Issue Description:

A denial of service vulnerability has been reported to exist in all hardware platforms that run Cisco IOS versions 11.x through 12.x. This issue may be triggered by a sequence of specifically crafted IPV4 packets. A power cycling of an affected device is required to regain normal functionality.

It is possible to block the remote router by sending malformed IPv4 packets.;
An attacker may use this flaw to render this router inoperable.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Cisco IOS and Unified Communications Manager Multiple Voice Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 6.8

CVE Reference: CVE-2007-4294

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95159
Bugtraq ID: 25239
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

Issue Description:

Cisco IOS and Cisco Unified Communications Manager are vulnerable to multiple denial of service and code execution issues. These issues arise because the application fails to handle malformed SIP packets. These vulnerabilities affect devices running Cisco IOS that have voice services enabled.

The successful exploitation of these vulnerabilities could lead to a denial of service condition or the execution of arbitrary code on a vulnerable device.

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to the following Cisco Security Advisory: Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager (Document ID 98182).

192.168.235.49 : Potential Vulnerabilities

Cisco IOS Secure Shell Server TACACS+ Multiple DoS (CSCed65778, CSCed65285)

Impact: Level 4 - Critical

CVE Reference: CVE-2005-1020, CVE-2005-1021

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 17988
BugTraq ID: 13042, 13043

Issue Description:

The remote device is missing a vendor-supplied security patch.

The remote version of IOS has the ability to enable an SSH server to let the administrators connect to the remote device.
There is an implementation flaw in the remote version of this software which may allow an attacker to cause a resource starvation on the remote device, thus preventing it from routing properly.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds
http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

Vulnerabilities in the Internet Key Exchange Xauth Implementation

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2005-1058

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 17986
Bugtraq ID: 13033, 13031
CVE ID: 2005-1058
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-04/0098.html
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

192.168.235.49 : Potential Vulnerabilities

Related OSVDB ID: 15304
Secunia Advisory ID: 14853
Security Tracker: 1013654
Vendor URL: http://www.cisco.com/

Issue Description:

The remote version of IOS contains a feature called Easy VPN Server which allows the administrator of the remote router to create a lightweight VPN server.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

Cisco Malformed SNMP Message Handling DoS (CSCdw67458)

Impact: Level 4 - Critical

CVE Reference: CVE-2002-0012, CVE-2002-0013

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10987
Bugtraq ID: 4088, 4132

Issue Description:

The remote device is missing a vendor-supplied security patch

There is a vulnerability in the way the remote device handles SNMP messages. An attacker may use this flaw to crash the remote device continuously.
This vulnerability is documented as Cisco bug ID CSCdw67458.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml

Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip)

Impact: Level 4 - Critical

192.168.235.49 : Potential Vulnerabilities

CVSS Score: 7.1

CVE Reference: CVE-2009-0630

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95154
Vendor Reference: http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

Issue Description:

A vulnerability exists in the handling of IP sockets that can cause devices to be vulnerable to a denial of service attack when any of the following features of Cisco IOS Software and Cisco IOS XE Software are enabled:
Cisco Unified Communications Manager Express
SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport
Secure Signaling and Media Encryption
Blocks Extensible Exchange Protocol (BEEP)
Network Admission Control HTTP Authentication Proxy
Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass
Distributed Director with HTTP Redirects
DNS (TCP mode only)

This vulnerability can be exploited by a remote attacker by sending specially-crafted TCP/IP packets to multiple TCP ports to prevent accepting new connections or sessions, exhaust memory, cause high CPU load, or to cause a reload of an affected device. (CVE-2009-0630)
For successful exploitation of this vulnerability, the TCP three-way handshake must be completed to the associated TCP port number for any of the features listed above.
Successful exploitation of the vulnerability may result in the any of the following occurring:
1) The configured feature may stop accepting new connections or sessions.
2) The memory of the device may be consumed.
3) The device may experience prolonged high CPU utilization.
4) The device may reload.

Suggestions:

- Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks.
- Use Receive ACL (rACL) to protect the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured.
- Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device.

Further information and examples on configuring iACLs, rACLs and CoPP can be found at the advisory cisco-sa-20090325-ip.
Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-ip for additional information on obtaining the fixes.

192.168.235.49 : Potential Vulnerabilities

Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels)

Impact: Level 3 - High

CVSS Score: 7.1

CVE Reference: CVE-2009-2872, CVE-2009-2873

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95227
http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml

Issue Description:

A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.
Devices that are running Cisco IOS Software and configured for GRE, IPinIP, Generic Packet Tunneling in IPv6 or IPv6 over IP tunnels tunnels and Cisco Express Forwarding may reload upon switching a specially crafted malformed packets. The Cisco IOS Point to Point Tunneling Protocol (PPTP) feature creates GRE tunnels that are transparent to the user. Therefore systems configured for PPTP are also vulnerable.

Successful exploitation of the vulnerability may result in the reload of an affected system, causing a denial of service.

Suggestions:

Solution:
Cisco has released an advisory detailing solutions available to fix the issue. Refer to Cisco Security Advisory cisco-sa-20090923-tunnels for additional information on obtaining the fixes.
Workarounds:
Disabling Cisco Express Forwarding will mitigate this vulnerability. It can be disabled in the following two ways:
1) Disable Cisco Express Forwarding Globally by using the no ip cef and no ipv6 cef global configuration commands.
2) Disable Cisco Express Forwarding on all Tunnel Interfaces configured on an affected device as shown in the following example:
interface Tunnel [interface-ID]
no ip route-cache cef
Impact of the workaround:
Disabling Cisco Express Forwarding may have significant performance impact and is not recommended by Cisco. Refer to the advisory for additional details on the workarounds.

192.168.235.49 : Potential Vulnerabilities

Cisco IOS NTP Daemon Buffer Overflow Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95226

Issue Description:

IOS is the router operating system maintained and distributed by Cisco Systems. Remote attackers can trigger a buffer overflow in the NTP daemon by sending a specially-crafted NTP control packet. The vulnerability is present whether the device is an NTP server or client, and may result in the execution of arbitrary code on the target machine.
For IOS, this issue is documented as Cisco Bug IDs CSCdt93866 and CSCdw35704.

The successful exploitation of this vulnerability could result in a buffer overflow and denial of service condition.

Suggestions:

Customers with service contracts should obtain upgraded software through their regular update channels for any software release containing the feature sets they have purchased. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Web site.

Cisco IOS Software TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24)

Impact: Level 3 - High

CVSS Score: 7.8

CVE Reference: CVE-2008-4609, CVE-2009-0627

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95241
http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml

192.168.235.49 : Potential Vulnerabilities

Issue Description:

Multiple Cisco products are affected by denial of service vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections.
By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.
Network devices are not directly impacted by TCP state manipulation denial of service attacks transiting a device; however, network devices that maintain the state of TCP connections may be impacted.

Successful exploitation of the TCP state manipulation vulnerabilities may result in a denial of service condition where new TCP connections are not accepted on an affected system. Repeated exploitation may result in a sustained denial of service condition.

Suggestions:

Patch:
Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco sa-20090908-tcp24 for additional information on obtaining the fixes.
Workarounds:
Cisco has guidelines for mitigation against the TCP state manipulation vulnerabilities for Cisco IOS Software, CatOS Software, ASA and PIX Software and Nexus Software. Please refer to Workaround Section at cisco-sa-20090908-tcp24 for detailed guidelines.

Cisco IOS TCLSH AAA Command Authorization Bypass

Impact: Level 3 - High

CVSS Score: 4.6

CVE Reference: CVE-2006-0485, CVE-2006-0486

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 20808
Bugtraq ID: 16383
CVE ID: 2006-0486, 2006-0485
FrSIRT Advisory: ADV-2006-0337
Related OSVDB ID: 34892, 22723
Secunia Advisory ID: 18613
Security Tracker: 1015543
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

192.168.235.49 : Potential Vulnerabilities

Issue Description:

The remote host is a CISCO router containing a version of IOS which is vulnerable to a remote AAA command autorization bypass vulnerability.

The remote version of IOS does not enforce AAA command authorization checks for commands etnered in the TCL shell. An attacker with a shell access on the remote route may gain elevated privileges on the remote device.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability

Impact: Level 3 - High

CVSS Score: 2.1

CVE Reference: CVE-2005-2451

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 19771
Bugtraq ID: 14414
CERT VU: 930892
CERT: TA05-210A
CVE ID: 2005-2451
ISS X-Force ID: 21591
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2005-07/0508.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-06/0558.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-06/0567.html
News Article: http://blog.washingtonpost.com/securityfix/2005/07/black_hat_day_1_update_on_cisc.html
News Article: http://www.news.com/2100-1002_3-5812044.html
News Article: http://www.wired.com/news/technology/0,1282,68435,00.html
Other Advisory URL: http://www.irmplc.com/index.php/69-Whitepapers
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/201
Secunia Advisory ID: 16272
Security Tracker: 1014598
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

Issue Description:

The remote version of IOS is vulnerable to a code execution vulnerability when processing malformed IPv6

192.168.235.49 : Potential Vulnerabilities

packets.

To exploit this flaw, an attacker would need to ability to send a malformed packet from a local segment and may exploit this issue to cause the remote device to reload repeatedly or to execute arbitrary code in the remote IOS.

Suggestions:

Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

Cisco IOS GRE Decapsulation Vulnerability

Impact: Level 2 - Medium

CVSS Score: 2.6

CVE Reference: CVE-2006-4650

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95148

Issue Description:

Cisco IOS is exposed to a vulnerability which can be exploited by malicious people to bypass certain security restrictions. This vulnerability is due to
an error within the handling of GRE packets with source routing information because the offset field is not verified before being used to decapsulate a packet.
The vulnerability affects Cisco IOS 12.0, 12.1, and 12.2 based trains when configured with GRE IP or GRE IP multipoint tunnels.

This vulnerability can be exploited to bypass certain security restrictions.

Suggestions:

Cisco released an advisory detailing various workarounds and solutions. Refer to the Cisco Security Advisory cisco-sr-20060906-gre for more information.

192.168.235.50 : Overview

Host Details

NETBIOS - Name
None
DNS - Reverse Record
None

192.168.235.50 : Vulnerabilities

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.50 :
69.164.210.215
207.192.75.2
209.123.10.29
209.123.10.26
209.123.10.78
213.200.73.121
89.149.184.182
4.68.110.77
4.68.16.126
4.69.134.117
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

192.168.235.51 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
Nokia IP130
PORT - Port/Protocol/Service/Banner Information
443/tcp(www) Apache
PORT - Port/Protocol/Service/Banner Information
22/tcp(ssh) SSH-1.99-OpenSSH_3.1p1
PORT - Port/Protocol/Service/Banner Information
23/tcp(telnet)

Open Ports

Port	Protocol	Service	Comment
22	tcp	ssh	Banner - SSH-1.99-OpenSSH_3.1p1
23	tcp	telnet	Banner - IPSO (nne) (ttyp0)
161	udp	snmp	Service - SNMP
443	tcp	https	Banner - Server: Apache
514	udp	syslog	Service - syslog

192.168.235.51 : Vulnerabilities

SSL 2.0 Protocol Usage

Impact: Level 5 - Urgent

CVSS Score: 5

CVE Reference: CVE-2005-2969

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 20007
http://www.schneier.com/paper-ssl.pdf
http://secunia.com/advisories/17151/
http://www.securiteam.com/securitynews/6Y00D0AEBW.html
http://devedge-temp.mozilla.org/viewsource/2001/tls-ssl3/
http://support.microsoft.com/kb/187498

Issue Description:

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

The vulnerability is caused due to an error in handling the use of "SSL_OP_MSIE_SSLV2_RSA_PADDING" option. The use of this option causes a verification check that prevents protocol-version rollback attacks to be disabled. This may be exploited in "man-in-the-middle" attacks to force a client and a server to negotiate the less secure SSL 2.0 protocol even when both parties support the more secure SSL 3.0 or TLS 1.0 protocols. The option is also enabled when the "SSL_OP_ALL" option is used.
Successful exploitation requires that SSL 2.0 is enabled, and either the "SSL_OP_MSIE_SSLV2_RSA_PADDING" or the "SSL_OP_ALL" option is used.

Suggestions:

Make sure to disable the SSL 2.0 protocol
OpenSSL 0.9.7 branch:
Update to version 0.9.7h or later.
OpenSSL 0.9.8 branch:
Update to version 0.9.8a or later.
IIS:
http://support.microsoft.com/kb/187498 or
http://support.microsoft.com/kb/245030/

SNMP Weak / Guessable Community String

192.168.235.51 : Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-2001-0514, CVE-2002-0109, CVE-2004-0311, CVE-2004-1473, CVE-2004-1474

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10264
Bugtraq ID: 11237, 2112, 9681, 6825, 177, 10576, 7081, 7212, 7317, 986
CERT VU: 329230
CVE ID: 1999-0517, 2004-0311, 1999-0254, 1999-0516, 1999-0186, 2004-1473
Generic Exploit URL: http://packetstormsecurity.nl/0402-exploits/apc_9606_backdoor.txt
Generic Informational URL: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Guessable_Read_Community.html&fact_color=doc&tag=
Generic Informational URL: http://www.securiteam.com/exploits/Patrol_s_SNMP_Agent_3_2_can_lead_to_root_compromise.html
Generic Informational URL: http://www.securiteam.com/exploits/Windows_NT_s_SNMP_service_vulnerability.html
ISS X-Force ID: 1240, 15238, 1387, 1241, 1385, 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0460.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0517.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0527.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Microsoft Knowledge Base Article: 99880
Other Advisory URL: http://cert.uni-stuttgart.de/archive/bugtraq/1998/11/msg00249.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/advise12
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 10905, 12635
Security Tracker: 1011388, 1011389
Snort Signature ID: 1411, 1412, 1413, 1414, 1892, 1893, 2406
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-22-00178-1&searchclause=00178
Vendor Specific Advisory URL: http://www.auscert.org.au/render.html?it=494
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1582
Vendor Specific Solution URL: http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch
Vendor Specific Solution URL: http://www.sun.com/solstice/products/ent.agents/
Vendor URL: http://www.apcc.com/
Vendor URL: http://www.managementsoftware.hp.com/
Vendor URL: http://www.symantec.com/

192.168.235.51 : Vulnerabilities

Issue Description:

The SNMP community string on the remote host is still set to the default or can easily be guessed.

Simple Network Management Protocol (SNMP) is used to remotely manage or monitor a host or network device. If an attacker is able to guess the read community string, an attacker will be able to freely view information like the operating system version, IP addresses, interfaces, processes/services, usernames, shares, etc. If the write community string is guessable an attacker has the ability to change system information, leading to anything from a partial to full compromise of the remote host.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community strings :
- public

Suggestions:

SNMP should preferably be removed if not in use.;;
Alternatively, the following security precautions should be put in place:;
- All community strings should be set to stronger, less easily guessable alternatives.;
- If SNMP is only used for monitoring purposes, write access should be disabled.;
- SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).;
- Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;;
For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:;
Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;

OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2006-5051, CVE-2006-5052 , CVE-2008-4109, CVE-2006-4924

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22466
Bugtraq ID: 20241, 20245
CVE ID: 2006-5051, 2008-4109, 2006-5052
ISS X-Force ID: 29254, 45202

192.168.235.51 : Vulnerabilities

Mail List Post: http://lists.debian.org/debian-security-announce/2008/msg00227.html
Other Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-527.htm
Other Advisory URL: http://www-unix.globus.org/mail_archive/security-announce/2007/04/msg00000.html
Other Advisory URL: http://www.debian.org/security/2008/dsa-1638
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1189
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1212
RedHat RHSA: RHSA-2006:0697-9, RHSA-2006:0698, RHSA-2006:0697
Secunia Advisory ID: 22173, 22196, 22183, 22236, 22158, 22208, 22245, 22270, 22362, 22352, 22487, 22495, 22823, 22926, 23680, 24805, 24799, 31885, 32080, 32181, 28320
Security Tracker: 1020891
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20061001-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=305214
Vendor Specific Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00004.html
Vendor Specific Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Oct/0005.html
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-216.htm
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200611-06.xml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:179
Vendor Specific Advisory URL: http://www.openbsd.org/errata.html#ssh
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-355-1
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-649-1
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=498678
Vendor Specific News/Changelog Entry: http://marc.theaimsgroup.com/?l=openbsd-cvs&m=115589252024127&w=2
Vendor Specific News/Changelog Entry: http://openssh.org/txt/release-4.4

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host contains a race condition that may allow an unauthenticated remote attacker to crash the service or, on portable OpenSSH, possibly execute code on the affected host.

In addition, another flaw exists that may allow an attacker to determine the validity of usernames on some platforms. Note that successful exploitation of these issues requires that GSSAPI authentication be enabled.

Suggestions:

Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org

Outdated SSH Protocol Versions Supported

Impact: Level 4 - Critical

CVE Reference: CVE-2001-0361, CVE-2001-1473 , CVE-2001-0572

192.168.235.51 : Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10882
Bugtraq ID: 2344
CERT VU: 61576, 997481, 888801, 161576
CIAC Advisory: I-047, m-017
CVE ID: 2001-0361, 2001-0572
Generic Informational URL: http://www.securityfocus.com/archive/1/161150
ISS X-Force ID: 6082
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2001-03/0225.html
Related OSVDB ID: 729
Snort Signature ID: 1324, 1325, 1326, 1327
Vendor Specific Advisory URL:
http://www.cisco.com/en/US/tech/tk583/tk617/technologies_security_advisory09186a00800b168e.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
Vendor Specific Advisory URL: http://www.debian.org/security/2001/dsa-027

Issue Description:

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Suggestions:

If you use OpenSSH, set the option 'Protocol' to '2'.
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.

CGI Generic SQL Injection (blind)

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42424
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://www.securitydocs.com/library/2651

Issue Description:

192.168.235.51 : Vulnerabilities

A CGI application hosted on the remote web server is potentially
prone to SQL injection attack.

By sending specially crafted parameters to one or more CGI scripts
hosted on the remote web server, Nessus was able to get a very
different response, which suggests that it may have been able to
modify the behavior of the application and directly access the underlying database.
An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify
the remote database, or even take control of the remote operating system.
Note that this script is experimental and may be prone to false positives.

Suggestions:

Modify the affected CGI scripts so that they properly escape
arguments.

IP Forwarding Enabled

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-1999-0511

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95149

Issue Description:

If this machine is not a router or a firewall, then IP forwarding should not be activated.

If this machine is not intended to be a router, then it may allow a malicious user to access your
internal network.

Suggestions:

Disable IP fowarding by following the appropriate instructions below:
On Windows 2000 and Windows NT, set the value of the following registry key to zero:
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParametersIPEnableRouter
On Linux, insert this line in your startup script: "sysctl -w net.ipv4.ip_forward=0"
On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup script: "ndd -set /dev/ip
ip_forwarding 0"
On Mac OS X, insert this line in your startup script: "sysctl -w net.inet.ip.forwarding=0"

192.168.235.51 : Vulnerabilities

Self-signed certificate

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95138

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers. By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

SSL Certificate Signed using Weak Hashing Algorithm

Impact: Level 3 - High

CVE Reference: CVE-2004-2761

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 35291
http://tools.ietf.org/html/rfc3279
http://www.phreedom.org/research/rogue-ca/
http://www.microsoft.com/technet/security/advisory/961509.mspx http://www.kb.cert.org/vuls/id/836068

192.168.235.51 : Vulnerabilities

Issue Description:

The remote service uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5.

These algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow him to masquerade as the affected service.

Suggestions:

Contact the Certificate Authority to have the certificate reissued.

Unencrypted Telnet Server

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 42263

Issue Description:

The remote Telnet server transmits traffic in cleartext.

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Suggestions:

Disable this service and use SSH instead.

Comments:

Created On: 2009-12-22 12:45:28
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across open networks such as the Internet.

192.168.235.51 : Vulnerabilities

SSL Medium Strength Cipher Suites Supported

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42873

Issue Description:

The remote service supports the use of medium strength SSL ciphers.

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Raw Scanner Output:

```
Plugin output :
Here are the medium strength SSL ciphers supported by the remote server :
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv2
      DES-CBC-MD5              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=MD5
      RC4-64-MD5               Kx=RSA       Au=RSA     Enc=RC4(64)
Mac=MD5
    SSLv3
      EDH-RSA-DES-CBC-SHA      Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
      DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
    TLSv1
      EDH-RSA-DES-CBC-SHA      Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
      EXP1024-DES-CBC-SHA      Kx=RSA(1024)  Au=RSA     Enc=DES(56)
Mac=SHA1   export
      EXP1024-RC4-MD5          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=MD5    export
      EXP1024-RC4-SHA          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=SHA1   export
      DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
The fields above are :
  {OpenSSL ciphername}
```

192.168.235.51 : Vulnerabilities

Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Suggestions:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95186

Issue Description:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

Raw Scanner Output:

```
GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.1
Host: 192.168.235.51
Connection: Keep-Alive
<form METHOD="POST" NAME="form"
ACTION="/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors"><font size=+2>
<b>Please Log
In</b> </font>
<BR>
<BR>
<TABLE BORDER=1>
<CAPTION><B></B></CAPTION>
<TR><TH></TH>
</TR><TD>
<b>User Name </b>
```

192.168.235.51 : Vulnerabilities

<TD>
<input type="TEXT" name="userName" SIZE="32"><TR>
<TD>
Password
<TD>
<input type="PASSWORD" name="userPass" SIZE="32"></TABLE>

Acquire Exclusive Configuration Lock
Yes
<INPUT TYPE="Radio" Checked Name="getLock" Value="t"> No
<INPUT TYPE="Radio" Name="getLock" Value="x">

<A HREF="/cgi-bin/login_adv.tcl" target="_top">Log In with Advanced
Options</A>

<HR SIZE=1>
<input type="image" border=0 src="/images/login.gif" name="Login"></form>

Suggestions:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

SSL Certificate - Signature Verification Failed Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95242

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:

192.168.235.51 : Vulnerabilities

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

CN does not match hostname

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95137

Weak Supported SSL Ciphers Suites

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 26928
The following links detail how to change the supported SSL Cipher Suites for IIS:;;
How to control the ciphers for SSL and TLS;
----------;
http://support.microsoft.com/kb/216482;;
How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll;
----------;
http://support.microsoft.com/kb/245030;;
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services;
----------;
http://support.microsoft.com/kb/187498;;
Apache;
----------;
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite;;

192.168.235.51 : Vulnerabilities

IBM HTTP Server;
----------;
ftp://ftp.software.ibm.com/software/webserver/appserv/library/v60/ihs_60.pdf;;
iPlanet;
----------;
http://docs.sun.com/source/816-5682-10/esecurty.htm#1008479;;
Note: It must be noted that these changes have not been tested by
SensePost, so the impact of these changes is unknown. The possibility exists that older Internet Browsing software may not be able to access the SSL protected portions of these websites, should they not have support for certain ciphers.;

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Weaker cyphers have a higher possibility of being cracked and as such it is recommended that 128bit cyphers be used, at a minimum.

Raw Scanner Output:

```
Plugin output :
Here is the list of weak SSL ciphers supported by the remote server :
  Low Strength Ciphers (< 56-bit key)
    SSLv2
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
The fields above are :
  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Suggestions:

192.168.235.51 : Vulnerabilities

Reconfigure the affected application if possible to avoid use of weak ciphers.

TCP Sequence Number Approximation

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-0230

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 12213
Bugtraq ID: 10183
CERT VU: 415294
CERT: CA-2001-09, TA04-111A
CVE ID: 2004-0230
FrSIRT Advisory: ADV-2006-3983
Generic Exploit URL: http://www.osvdb.org/ref/04/04030-exploit.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/disconn.py
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/Kreset.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp_rfc31337-compliant.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/tcp_reset.c
Generic Exploit URL: http://www.packetstormsecurity.org/0405-exploits/autoRST.c
Generic Exploit URL: http://www.packetstormsecurity.org/cisco/ttt-1.3r.tar.gz
Generic Informational URL: http://nytimes.com/aponline/technology/AP-Internet -Threat.html
Generic Informational URL:
http://slashdot.org/articles/04/04/20/1738217.shtml?tid=126&tid=128&tid=172&tid=95
Generic Informational URL: http://www.cnn.com/2004/TECH/internet/04/20/internet.threat/index.html
Generic Informational URL: http://www.eweek.com/article2/0,1759,1571185,00.asp
Generic Informational URL: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
Generic Informational URL: http://www.ietf.org/rfc/rfc0793.txt
Generic Informational URL: http://www.msnbc.msn.com/id/4788445/
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.ppt
ISS X-Force ID: 15886
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0028.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0029.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108302060014745&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108506952116653&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
Microsoft Knowledge Base Article: 922819

192.168.235.51 : Vulnerabilities

Microsoft Security Bulletin: MS05-019
Microsoft Security Bulletin: MS06-064
Other Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3/SCOSA-2005.3.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9/SCOSA-2005.9.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Other Advisory URL: http://www.jpcert.or.jp/at/2004/at040003.txt
Other Advisory URL: http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx
Other Advisory URL: http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
Other Advisory URL: http://www.seil.jp/en/ann/announce_en_20040421_01.txt
Other Advisory URL: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Other Advisory URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/170
Other Solution URL: http://isc.sans.org/diary.php?date=2004-04-20
OVAL ID: 4791, 2689, 3508, 270
Related OSVDB ID: 6094, 29429, 4030
Secunia Advisory ID: 11448, 11447, 11443, 11444, 11445, 11462, 11458, 11682, 11679, 12682, 14946, 22341, 14170, 11440
Snort Signature ID: 2523
US-CERT Cyber Security Alert: TA04-111A
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2005.05.02.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
Vendor Specific Advisory URL: http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
Vendor Specific Advisory URL: http://www.juniper.net/support/alert.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/niscc-236929.txt
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1535
Vendor Specific Advisory URL: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
Vendor Specific News/Changelog Entry: http://www.juniper.net/support/alert.html
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc

Issue Description:

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc.).

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST

packet into the session, causing it to be reset and effectively allowing for denial of service attacks.

Suggestions:

Please see http://www.securityfocus.com/bid/10183/solution, for the right solution for your infrastructure.

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Impact: Level 2 - Medium

CVSS Score: 6.4

CVE Reference: CVE-2009-3555

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42880
http://extendedsubset.com/?p=8
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.kb.cert.org/vuls/id/120541
http://www.g-sec.lu/practicaltls.pdf
https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt
BID:36935
OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974

Issue Description:

The remote service allows renegotiation of TLS / SSL connections.

Suggestions:

No suggestion at this time

Telnet Service and Version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

192.168.235.51 : Vulnerabilities

Other References:

Nessus NASL ID : 10281

Issue Description:

This detects the Telnet server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and types should be omitted where possible.

Raw Scanner Output:

Plugin output :
Here is the banner from the remote Telnet server :
---------- snip ----------
IPSO (nne) (ttyp0)
login:
---------- snip ----------

Suggestions:

Informational plugin.

CGI's Found

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10662

Issue Description:

This script makes a mirror of the remote web site(s)and extracts the list of CGIs that are used by the remote host. Please refer to 'details' for more information.

Raw Scanner Output:

Plugin output :

192.168.235.51 : Vulnerabilities

The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/cgi-bin (userPass [] userName [] getLock [x] Login [])
/cgi-bin/home.tcl (userPass [] userName [] overrideLock [t] getLock [x]
Login [])

Suggestions:

Informational plugin.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Apache
and the 'ServerTokens' directive is ProductOnly
Apache does not offer a way to hide the server type.

Suggestions:

Informational plugin.

Supported SSL Ciphers Suites

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.51 : Vulnerabilities

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 21643
http://www.openssl.org/docs/apps/ciphers.html

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Raw Scanner Output:

```
Plugin output :
Here is the list of SSL ciphers supported by the remote server :
  Low Strength Ciphers (< 56-bit key)
    SSLv2
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv2
      DES-CBC-MD5              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=MD5
      RC4-64-MD5               Kx=RSA       Au=RSA     Enc=RC4(64)
Mac=MD5
    SSLv3
      EDH-RSA-DES-CBC-SHA      Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
      DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
    TLSv1
      EDH-RSA-DES-CBC-SHA      Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
```

192.168.235.51 : Vulnerabilities

```
    EXP1024-DES-CBC-SHA       Kx=RSA(1024)  Au=RSA     Enc=DES(56)
Mac=SHA1   export
    EXP1024-RC4-MD5           Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=MD5    export
    EXP1024-RC4-SHA           Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=SHA1   export
    DES-CBC-SHA               Kx=RSA        Au=RSA     Enc=DES(56)
Mac=SHA1
  High Strength Ciphers (>= 112-bit key)
   SSLv2
    DES-CBC3-MD5              Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=MD5
    RC4-MD5                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
   SSLv3
    EDH-RSA-DES-CBC3-SHA      Kx=DH         Au=RSA     Enc=3DES(168)
Mac=SHA1
    DES-CBC3-SHA              Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
    RC4-MD5                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
    RC4-SHA                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1
   TLSv1
    EDH-RSA-DES-CBC3-SHA      Kx=DH         Au=RSA     Enc=3DES(168)
Mac=SHA1
    DES-CBC3-SHA              Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
    RC4-MD5                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
    RC4-SHA                   Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1
The fields above are :
 {OpenSSL ciphername}
 Kx={key exchange}
 Au={authentication}
 Enc={symmetric encryption method}
 Mac={message authentication code}
 {export flag}
```

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

IP protocols scan

Impact: Level 1 - Low

192.168.235.51 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

Traceroute

192.168.235.51 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.51 :
69.164.210.215
207.192.75.2
209.123.10.29
209.123.10.102
209.123.10.74
213.200.73.121
89.149.187.246
4.68.110.77
4.68.16.62
4.69.134.113
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.51

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

TCP timestamps

192.168.235.51 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

192.168.235.51 : Vulnerabilities

Plugin output :
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
Date: Mon, 07 Dec 2009 23:48:51 GMT
Server: Apache
Set-Cookie: Session=Login
path=/
Cache-Control: no-chache
Expires: -1
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

Remote Access or Management Service Detected

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95236

Issue Description:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks. The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin) and VNC are checked.

Consequences vary by the type of attack.

Raw Scanner Output:

192.168.235.51 : Vulnerabilities

Service name: SSH on TCP port 22.
Service name: Telnet on TCP port 23.

Suggestions:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A telnet server is running on this port.

Suggestions:

Informational plugin.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

192.168.235.51 : Vulnerabilities

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Synopsis :
It is possible to determine the exact time set on the remote host.
Description :
The remote host answers to an ICMP timestamp request. This allows an
attacker to know the date which is set on your machine.
This may help him to defeat all your time based authentication
protocols.
Solution :
Filter out the ICMP timestamp requests (13), and the outgoing ICMP
timestamp replies (14).
Risk factor :
None
Plugin output :
The ICMP timestamps seem to be in little endian format (not in network
format)
The difference between the local and remote clocks is 3088 seconds.
CVE : CVE-1999-0524

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

192.168.235.51 : Vulnerabilities

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port through SSLv2.

Suggestions:

Informational plugin.

SSL Certificate Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10863

Issue Description:

The scanner was able to determine what SSL ciphers are supported by the server.

The use of weak ciphers may lead to the compromise of data in transit.

Raw Scanner Output:

Synopsis :
This plugin displays the SSL certificate.
Description :
This plugin connects to every SSL-related port and attempts to
extract and dump the X.509 certificate.
Solution :
n/a
Risk factor :
None
Plugin output :

192.168.235.51 : Vulnerabilities

Subject Name:
Country: CA
State/Province: Ontario
Locality: Ottawa
Organization: EWA-Canada
Organization Unit: ASVV Lab
Common Name: nne
Email Address: noc@ewa-canada.com
Issuer Name:
Country: CA
State/Province: Ontario
Locality: Ottawa
Organization: EWA-Canada
Organization Unit: ASVV Lab
Common Name: nne
Email Address: noc@ewa-canada.com
Serial Number: 00 9D 32 83
Version: 1
Signature Algorithm: MD5 With RSA Encryption
Not Valid Before: Mar 02 15:44:20 2009 GMT
Not Valid After: Mar 02 15:44:20 2010 GMT
Public Key Info:
Algorithm: RSA Encryption
Public Key: 00 BF 3A EA CA 07 70 68 2C B9 56 B9 EF 6D E5 2F 79 23 62 30
16 3D 03 46 17 73 B3 11 2E 57 C5 D1 76 B7 65 25 18 68 7F 66
5A 67 E5 05 C4 68 99 46 07 9E 0F 3E B7 FA 7D EC 97 94 B8 69
2D A2 B0 C9 D9 05 5D EE 6E 67 94 0B 5A 48 67 24 FC D8 BE 38
D9 95 17 9C 1B 9E 16 B5 9E 20 5F FE 9A BB 01 09 ED 00 32 30
F7 44 1A 88 65 0B A4 C4 8E 32 B5 FC AF AC FB E2 7D F5 B6 77
F3 D8 6D 66 0B 60 06 D5 5B
Exponent: 01 00 01
Signature: 00 45 55 56 00 BF A8 9C 18 2A 7A C7 7F 84 8C B3 58 0B 3D E5
3C 84 95 C1 66 DE 96 3C 55 8A 7E E3 53 9D 0B 75 1B 9D 4A B2
1C 0C 06 AA E8 E8 14 61 BE 7D 18 50 32 8C 08 9E A8 F7 3D E3
CE 9D 36 9B 06 D9 E8 51 B1 DB 82 DE 44 0A 9F 55 95 E4 B1 60
02 C8 AF 89 EA 6D FC 1A 63 54 3B 90 FB 2B 94 EB D7 C1 07 82
D9 DB B9 98 27 3A F6 13 30 BD AC BB CB F5 8B 12 54 64 A2 4F
AE F8 CE 9F F9 9D 2D D5 AA

Suggestions:

Informational plugin.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.51 : Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-1.99-OpenSSH_3.1p1
SSH supported authentication : publickey,password,keyboard-interactive

Suggestions:

Informational plugin.

HTTP Cookies

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 39463

Issue Description:

Some cookies have been set by the web server.

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser. As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions. This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

Raw Scanner Output:

192.168.235.51 : Vulnerabilities

Plugin output :
path = /
name = Session
value = Login
version = 1
secure = 0
httponly = 0

Suggestions:

Informational plugin.

Friendly HTTP Error Messages Detected

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10386

Issue Description:

Some web servers are configured in that they do not return '404 Not Found' error codes when a non-existent file is requested perhaps returning a site map, authentication page or search page instead.

This script will retrieve the default page which is issued when a non-existent file is requested and will use this information to minimize the risk of reporting "False Positives"

Suggestions:

If a great number of security holes are produced for this port, they might not all be accurate.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

192.168.235.51 : Vulnerabilities

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : SCO UnixWare 7.1.1
Confidence Level : 65
Method : SinFP
The remote host is running SCO UnixWare 7.1.1

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSLv2 server answered on this port.

192.168.235.51 : Vulnerabilities

Suggestions:

Informational plugin.

SSH Protocol Versions Supported.

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Synopsis :
A SSH server is running on the remote host.
Description :
This plugin determines the versions of the SSH protocol supported by
the remote SSH daemon.
Solution :
n/a
Risk factor :
None
Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
- 1.33
- 1.5
- 1.99
- 2.0
SSHv1 host key fingerprint :
4a:2a:ee:10:26:62:32:08:25:94:fe:6b:05:db:47:26
SSHv2 host key fingerprint :
1f:c7:50:9d:af:cc:cd:aa:fe:5d:f7:34:c5:ca:d8:e8

Suggestions:

Informational plugin.

192.168.235.51 : Potential Vulnerabilities

SSH version older than 3.4

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2002-0639, CVE-2002-0640

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11031
Bugtraq ID: 5093
CERT VU: 69347
CERT: CA-2002-18
CIAC Advisory: m-095
CVE ID:2002-0640, 2002-0639
Generic Informational URL: http://www.net-security.org/vuln.php?id=1817
ISS X-Force ID: 9169
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2002-06/0294.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2002-06/0376.html
Other Advisory URL: http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20584
RedHat RHSA: RHSA-2002:127-25
Related OSVDB ID: 839, 6245
Snort Signature ID: 1810, 1811, 1812
Vendor Specific Advisory URL: ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-030.0.txt
Vendor Specific Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:31.openssh.asc
Vendor Specific Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SN-02:05.asc
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-005.txt.asc
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000500
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000502
Vendor Specific Advisory URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F45508&zone_32=category%3Asecurity
Vendor Specific Advisory URL: http://www.debian.org/security/2002/dsa-134
Vendor Specific Advisory URL: http://www.globalintersec.com/adv/openssh-2002062801.txt
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/other_advisory-2157.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/other_advisory-2162.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/other_advisory-2177.html
Vendor Specific Advisory URL: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:040
Vendor Specific Advisory URL: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:040-1
Vendor Specific Advisory URL: http://www.openpkg.org/security/OpenPKG-SA-2002.005-openssh.html
Vendor Specific Advisory URL: http://www.openssh.com/txt/iss.adv

192.168.235.51 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://www.openssh.com/txt/preauth.adv
Vendor Specific Advisory URL: http://www.suse.com/de/security/2002_024_openssh_txt.html
Vendor Specific Advisory URL: http://www.suse.com/de/security/openssh_2_txt.html
Vendor Specific Advisory URL: http://www.suse.de/de/security/2002_024_openssh_txt.html
Vendor Specific Advisory URL: http://www.trustix.net/errata/misc/2002/TSL-2002-0059-openssh.asc.txt
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2002-127.html
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2002-131.html
Vendor URL: http://www.openssh.com/

Issue Description:

You are running a version of OpenSSH which is older than 3.4

There is a flaw in this version that can be exploited remotely to
give an attacker a shell on this host.
Note that several distribution patched this hole without changing
the version number of OpenSSH. Since Nessus solely relied on the
banner of the remote SSH server to perform this check, this might
be a false positive.
If you are running a RedHat host, make sure that the command :
rpm -q openssh-server
Returns :
openssh-server-3.1p1-6

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

OpenSSH Buffer Management Vulnerability (OpenSSH < 3.7.1)

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2003-0682, CVE-2003-0693, CVE-2003-0695

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11837
Bugtraq ID: 8628
CERT VU: 333628
CERT: CA-2003-24
CIAC Advisory: N-151, o-030
CVE ID: 2003-0695, 2003-0693, 2003-0682
ISS X-Force ID: 13191, 13214

192.168.235.51 : Potential Vulnerabilities

Other Advisory URL: http://archives.neohapsis.com/archives/fulldisclosure/2003-q3/3967.html
Other Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106373247528528&w=2
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/144
RedHat RHSA: RHSA-2003:279, RHSA-2003:280, RHSA-2003:222
Secunia Advisory ID: 9743, 10156, 9747, 9756, 9744, 9810, 9811
Security Tracker: 1007716
Vendor Specific Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:12.openssh.asc
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-012.txt.asc
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-027.0.txt
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20030904-02-P.asc
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20031001-01-U.asc
Vendor Specific Advisory URL: http://cc.turbolinux.com/security/TLSA-2003-51.txt
Vendor Specific Advisory URL: http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000741
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/index.php?id=a&anuncio=000739
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/index.php?id=a&anuncio=000741
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=61798
Vendor Specific Advisory URL: http://infocenter.guardiandigital.com/knowledgebase/123
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106381396120332&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106381409220492&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106382542403716&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=openbsd-security-announce&m=106375582924840
Vendor Specific Advisory URL: http://security.debian.org/pool/updates/main/o/openssh-krb5/ssh-krb5_3.4p1-0woody4_hppa.deb
Vendor Specific Advisory URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56861&zone_32=category%3Asecurity
Vendor Specific Advisory URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56862&zone_32=category%3Asecurity
Vendor Specific Advisory URL: http://support.f-secure.com/enu/corporate/supportissue/ssh/comments/comments-issue-2003120401.shtml
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2003.1217.1
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1500.1
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0100.1
Vendor Specific Advisory URL: http://www.bluecoat.com/downloads/support/BCS_OpenSSH_vulnerability.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_openSSH_buffer_vulnerability.html
Vendor Specific Advisory URL: http://www.caldera.com/support/security/2003.html#OpenServer
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml
Vendor Specific Advisory URL: http://www.debian.org/security/2003/dsa-382
Vendor Specific Advisory URL: http://www.debian.org/security/2003/dsa-383
Vendor Specific Advisory URL: http://www.foundrynet.com/solutions/advisories/openssh333628.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/openssh_1.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/engarde_advisory-3621.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/engarde_advisory-3649.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/gentoo_advisory-3629.html

192.168.235.51 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/immunix_advisory-3627.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/immunix_advisory-3635.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/slackware_advisory-3639.html
Vendor Specific Advisory URL: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:090-1
Vendor Specific Advisory URL: http://www.mindrot.org/pipermail/openssh-unix-announce/2003-September/000064.html
Vendor Specific Advisory URL: http://www.netscreen.com/services/security/alerts/openssh_1.jsp
Vendor Specific Advisory URL: http://www.openbsd.org/errata33.html#sshbuffer
Vendor Specific Advisory URL: http://www.openpkg.org/security/OpenPKG-SA-2003.040-openssh.html
Vendor Specific Advisory URL: http://www.openssh.com/txt/buffer.adv
Vendor Specific Advisory URL: http://www.riverstonenet.com/support/tb0265-9.html
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.368193
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.373294
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.374735
Vendor Specific Advisory URL: http://www.suse.com/de/security/2003_039_openssh.html
Vendor Specific Advisory URL: http://www.suse.de/de/security/2003_038_openssh.html
Vendor Specific Advisory URL: http://www.suse.de/de/security/2003_039_openssh.html
Vendor Specific Advisory URL: http://www.trustix.net/errata/misc/2003/TSL-2003-0033-openssh.asc.txt
Vendor Specific Advisory URL: http://www.trustix.org/pipermail/tsl-discuss/2003-September/007507.html
Vendor Specific Advisory URL: http://www.vmware.com/download/esx/esx152-patch5.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1371
Vendor Specific Advisory URL: https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=3D
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-222.html
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-279.html
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-280.html
Vendor Specific Advisory URL: https://www.ingrian.com/support/iwsc/security.php
Vendor Specific Advisory URL: https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2003-09-007&actionBtn=Search
Vendor Specific News/Changelog Entry: http://www116.nortel.com/docs/bvdoc/alteon/ssl/iSD-SSL_3.1.6.14_README.pdf
Vendor Specific Solution URL: ftp://ftp.openpkg.org/release/1.3/UPD/
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.24
Vendor Specific Solution URL: http://download.bluecoat.com/release/SGOS/index.html
Vendor Specific Solution URL: http://download.bluecoat.com/release/SGOS3/index.html
Vendor Specific Solution URL: http://oss.software.ibm.com/developerworks/projects/opensshi
Vendor Specific Solution URL: http://security.debian.org/pool/updates/main/o/openssh-krb5/ssh-krb5_3.4p1-0woody4_i386.deb
Vendor Specific Solution URL: http://sunsolve.sun.com/cobalt
Vendor Specific Solution URL: http://sunsolve.sun.com/patches/linux/security.html
Vendor Specific Solution URL: http://vmware-svca.www.conxion.com/secured/esx/esx-1.5.2-patch5.tar.gz
Vendor Specific Solution URL: http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
Vendor Specific Solution URL: http://www.cisco.com/tacpage/sw-center/
Vendor Specific Solution URL: http://www.cyclades.com/support/downloads.php
Vendor Specific Solution URL: http://www.f-secure.com/webclub/ssh/

192.168.235.51 : Potential Vulnerabilities

Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120244
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120245
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120246
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120247
Vendor Specific Solution URL: http://www.mandrakesecure.net/en/ftp.php
Vendor Specific Solution URL: http://www.netscreen.com/cso
Vendor Specific Solution URL: http://www.riverstonenet.com/support/support_sw_download.shtml
Vendor Specific Solution URL: http://www.trustix.net/pub/Trustix/updates/
Vendor Specific Solution URL: https://www.ingrian.com/suppport
Vendor URL: http://www.openssh.com/

Issue Description:

OpenSSH's SSH Daemon prior to 3.7.1 contains buffer management errors, which depending on factors such as the underlying operating system might allow an attacker to execute arbitrary commands on this host. Other implementations sharing common origin may also have these issues.
An exploit for this issue is rumoured to exist.

Buffer management problems have been found in all versions of OpenSSH's SSH daemon which are potentially remotely exploitable. Rumours currently exist of exploits in the wild for this bug against Linux on the intel platform. This vulnerability even extends to network devices using the OpenSSH implementation.
According to Cisco, devices currently vulnerable to the DoS condition include :
Cisco Catalyst Switching Software (CatOS)
CiscoWorks 1105 Hosting Solution Engine (HSE)
CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
Cisco SN 5428 Storage Router

Suggestions:

This issue is resolved in OpenSSH releases 3.7.1 and later. Upgrade to latest stable release version of OpenSSH available from www.openssh.com. Manual patches for this issue are available from http://www.openssh.com/txt/buffer.adv.
For vendor specific patch information, look up the vendor in question from http://www.securityfocus.com/bid/8628/solution, or contact the vendor directly.

OpenSSH < 5.0

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2000-0999, CVE-2001-0572, CVE-2001-1029, CVE-2005-2797, CVE-2005-2798, CVE-2006-0225, CVE-2006-4924, CVE-2006-4925, CVE-2006-5051, CVE-2006-5052, CVE-2006-5229, CVE-2006-5794, CVE-2007-2243, CVE-2007-3102, CVE-2007-4752, CVE-2008-1483, CVE-2008-1657, CVE-2008-3234, CVE-2008-3259, CVE-2008-4109, CVE-2008-5161

192.168.235.51 : Potential Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95134

Issue Description:

OpenSSH version is older than 5.0.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.0, is below:
CVE-2000-0999 - OpenBSD ssh Format String Privilege Escalation
CVE-2001-0572 - Cisco Devices SSH Password Length Disclosure, SSH Traffic Analysis Connection Attributes Disclosure
CVE-2001-1029 - OpenSSH on FreeBSD libutil Arbitrary File Read
CVE-2005-2797 - OpenSSH Multiple X11 Channel Forwarding Leaks
CVE-2005-2798 - OpenSSH GSSAPIAuthentication Credential Escalation
CVE-2006-0225 - OpenSSH scp Command Line Filename Processing Command Injection
CVE-2006-4924 - OpenSSH Identical Block Packet DoS
CVE-2006-4925 - OpenSSH packet.c Invalid Protocol Sequence Remote DoS
CVE-2006-5051 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2006-5052 - OpenSSH GSSAPI Authentication Abort Username Enumeration
CVE-2006-5229 - OpenSSH Username Password Complexity Account Enumeration
CVE-2006-5794 - OpenSSH Privilege Separation Monitor Weakness
CVE-2007-2243 - OpenSSH S/KEY Authentication Account Enumeration
CVE-2007-3102 - OpenSSH linux_audit_record_event Crafted Username Audit Log Injection
CVE-2007-4752 - OpenSSH Trusted X11 Cookie Connection Policy Bypass
CVE-2008-1483 - OpenSSH X11 Forwarding Local Session Hijacking
CVE-2008-1657 - OpenSSH ~/.ssh/rc ForceCommand Bypass Arbitrary Command Execution
CVE-2008-3234 - OpenSSH on Debian sshd Crafted Username Arbitrary Remote SELinux Role Access
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
CVE-2008-4109 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2008-5161 - OpenSSH CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure, SSH Tectia Multiple Products CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: www.openssh.org

OpenSSH < 4.0

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2001-0872, CVE-2001-1507, CVE-2002-0083, CVE-2002-0575,

CVE-2002-0639, CVE-2002-0640, CVE-2002-0765, CVE-2003-0190, CVE-2003-0386, CVE-2003-0682, CVE-2003-0693, CVE-2003-0695, CVE-2003-0786, CVE-2003-0787, CVE-2003-1562, CVE-2004-0175, CVE-2004-1653, CVE-2004-2069, CVE-2004-2760, CVE-2005-2666, CVE-2005-2798, CVE-2006-0225, CVE-2006-0883, CVE-2006-4924, CVE-2006-5051, CVE-2006-5052, CVE-2007-2243, CVE-2007-4654, CVE-2008-3259, CVE-2008-4109

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95133

Issue Description:

OpenSSH version is older than 4.0.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 4.0, is below:
CVE-2001-0872 - OpenSSH UseLogin Environment Variable Local Command Execution
CVE-2001-1507 - OpenSSH with KerberosV Remote Authentication Bypass
CVE-2002-0083 - OpenSSH Channel Code Off by One Privilege Escalation
CVE-2002-0575 - OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
CVE-2002-0639 - OpenSSH SKEY/BSD_AUTH Challenge-Response Remote Overflow
CVE-2002-0640 - OpenSSH PAMAuthenticationViaKbdInt Challenge-Response Remote Overflow
CVE-2002-0765 - OpenSSH YP Netgroups Authentication Bypass
CVE-2003-0190 - OpenSSH Root Login Timing Side-Channel Weakness, OpenSSH w/ PAM Username Validity Timing Attack
CVE-2003-0386 - OpenSSH Reverse DNS Lookup Bypass
CVE-2003-0682 - OpenSSH *realloc() Unspecified Memory Errors
CVE-2003-0693 - OpenSSH buffer_append_space() Heap Corruption
CVE-2003-0695 - OpenSSH Multiple Buffer Management Multiple Overflows
CVE-2003-0786 - OpenSSH SSHv1 PAM Challenge-Response Authentication Privilege Escalation
CVE-2003-0787 - OpenSSH PAM Conversation Function Stack Modification
CVE-2003-1562 - OpenSSH Root Login Timing Side-Channel Weakness, OpenSSH w/ PAM Username Validity Timing Attack
CVE-2004-0175 - OpenSSH scp Traversal Arbitrary File Overwrite
CVE-2004-1653 - OpenSSH Default Configuration Anon SSH Service Port Bounce Weakness
CVE-2004-2069 - OpenSSH Privilege Separation LoginGraceTime DoS
CVE-2004-2760 - OpenSSH sshd TCP Connection State Remote Account Enumeration
CVE-2005-2666 - Multiple SSH known_hosts Plaintext Host Disclosure
CVE-2005-2798 - OpenSSH GSSAPIAuthentication Credential Escalation
CVE-2006-0225 - OpenSSH scp Command Line Filename Processing Command Injection
CVE-2006-0883 - OpenSSH with OpenPAM Connection Saturation Forked Process Saturation DoS
CVE-2006-4924 - OpenSSH Identical Block Packet DoS
CVE-2006-5051 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2006-5052 - OpenSSH GSSAPI Authentication Abort Username Enumeration

192.168.235.51 : Potential Vulnerabilities

CVE-2007-2243 - OpenSSH S/KEY Authentication Account Enumeration
CVE-2007-4654 - Cisco WebNS SSHield w/ OpenSSH Crafted Large Packet Remote DoS
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
CVE-2008-4109 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: www.openssh.org

OpenSSH Reverse DNS Lookup bypass

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2003-0386

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11712
Bugtraq ID: 7831
CERT VU: 978316
CVE ID: 2003-0386
ISS X-Force ID: 12196
Mail List PostL http://archives.neohapsis.com/archives/bugtraq/2003-06/0038.html
RedHat RHSA: RHSA-2006:0298, RHSA-2006:0698
Secunia Advisory ID: 8974, 21129, 21262, 21724, 22196, 23680
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20060703-01-U.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=61798
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-174.htm
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1534
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html

Issue Description:

You are running OpenSSH 3.6.1 (portable) or older. There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of the target server.

OpenSSH features a mecanism which can restrict the list of hosts a given user can log from by specifying pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network). However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mecanism.

192.168.235.51 : Potential Vulnerabilities

Suggestions:

Upgrade to the latest stable release version of OpenSSH, available from http://www.openssh.org. This problem is resolved in OpenSSH 3.6.2 and later.

OpenSSH AFS/Kerberos ticket/token passing

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2002-0575

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10954
Bugtraq ID: 4560
CVE ID: 2002-0575
ISS X-Force ID: 8896
Vendor Specific Advisory URL: http://lists.trustix.org/pipermail/tsl-announce/2002-April/000089.html
Vendor Specific Advisory URL: http://lists.virus.org/openssh-announce-0204/msg00001.html
Vendor URL: http://www.openssh.org/security.html

Issue Description:

You are running a version of OpenSSH older than OpenSSH 3.2.1

A buffer overflow exists in the daemon if AFS is enabled on
your system, or if the options KerberosTgtPassing or
AFSTokenPassing are enabled. Even in this scenario, the
vulnerability may be avoided by enabling UsePrivilegeSeparation.
Versions prior to 2.9.9 are vulnerable to a remote root
exploit. Versions prior to 3.2.1 are vulnerable to a local
root exploit.

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

Expect Header Cross-Site Scripting Vulnerability

Impact: Level 3 - High

192.168.235.51 : Potential Vulnerabilities

CVE Reference: CVE-2006-3918, CVE-2007-5944

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22254
Bugtraq ID: 26457
CVE ID: 2006-3918, 2007-5944
FrSIRT Advisory: ADV-2006-2963, ADV-2006-2964, ADV-2007-3680
RedHat RHSA: RHSA-2006:0618, RHSA-2006:0692
Secunia Advisory ID: 21172, 21399, 1016569, 21478, 21598, 21744, 21848, 21986, 22140, 22317, 22523, 28749, 29640, 27674
Security Tracker: 1018963
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P.asc
Vendor Specific Advisory URL: http://openbsd.org/errata.html#httpd2
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-194.htm
Vendor Specific Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg24013080
Vendor Specific Advisory URL: http://www.us.debian.org/security/2006/dsa-1167
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=394965
Vendor Specific News/Changelog Entry: http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
Vendor URL: http://httpd.apache.org/

Issue Description:

The remote web server fails to sanitize the contents of an 'Expect' request header before using it to generate dynamic web content.

An unauthenticated remote attacker may be able to leverage this issue to launch cross-site scripting attacks against the affected service, perhaps through specially-crafted ShockWave (SWF) files.

Suggestions:

Check with the vendor for an update to the web server. For Apache, the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2. For IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1. For IBM WebSphere Application Server, upgrade to 5.1.1.17.

OpenSSH X11 Session Hijacking Vulnerability

Impact: Level 3 - High

CVE Reference: CVE-2008-1483

Port/Protocol: 22/TCP

192.168.235.51 : Potential Vulnerabilities

Other References:

Nessus NASL ID : 31737
Bugtraq ID: 28444
Secunia Advisory ID 229522, 29537, 29554, 29626, 29627, 29676, 29683, 29686, 29721, 29735, 29873, 29939, 30086, 30230, 30249, 30347, 30361, 31531, 31882
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01462841
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3137
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
Vendor Specific News/Changelog Entry: http://sourceforge.net/project/shownotes.php?release_id=590180

Issue Description:

According to its banner, the version of SSH installed on the remote host is older than 5.0.

Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

Suggestions:

Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org

Netscape/OpenSSL Cipher Forcing Bug

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95188

Issue Description:

Netscape's SSLv3 implementation had a bug where if a SSLv3 connection is initially established, the first available cipher is used. If a session is
resumed, a different cipher may be chosen if it appears in the passed cipher list before the session's current cipher. This bug can be used to change ciphers on the server.
OpenSSL contains this bug if the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option is enabled during runtime. This option was introduced for compatibility reasons.
The problem arises when different applications using OpenSSL's libssl library enable all compatibility

192.168.235.51 : Potential Vulnerabilities

options including SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG, thus enabling the bug.

A malicious legitimate client can enforce a ciphersuite not supported by the server to be used for a session between the client and the server. This can result in disclosure of sensitive information.

Suggestions:

This problem can be fixed by disabling the SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG option from the options list of OpenSSL's libssl
library. This can be done by replacing the SSL_OP_ALL definition in the openssl/ssl.h file with the following line:
#define SSL_OP_ALL (0x00000FFFL^SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG)
The library and all programs using this library need to be recompiled to ensure that the correct OpenSSL library is used during linking.

OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056)

Impact: Level 3 - High

CVSS Score: 4.6

CVE Reference: CVE-2006-0225

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95233
BugTraq ID: 16369
http://www.openssh.com/
http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00062.html
http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
http://www.vmware.com/support/vi3/doc/esx-3069097-patch.html

Issue Description:

OpenSSH is a freely available, open source implementation of the Secure Shell protocol. It is available for multiple platforms, including Unix, Linux and Microsoft. SCP is a secure copy application that is a part of OpenSSH. It is used to copy files from one computer to another over an SSH connection. If SCP is given all-local paths to copy, it acts like the system "cp" command.
OpenSSH is susceptible to a local SCP shell command execution vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input prior to utilizing it in a "system()" function call.
If SCP is used in an all-local fashion, without any hostnames, it utilizes the "system()" function to execute a local copy operation. By utilizing the "system()" function, a shell is spawned to process the arguments. If filenames are created that contain shell metacharacters, they will be processed by the

shell during the "system()" function call. Attackers can create files with names that contain shell metacharacters along with commands to be executed. If a local user then utilizes SCP to copy these files (likely during bulk copy operations involving wildcards), then the attacker-supplied commands will be executed with the privileges of the user running SCP.
This issue reportedly affects OpenSSH Version 4.2. Other versions may also be affected.

This issue can allow local attackers to execute arbitrary shell commands with the privileges of users executing a vulnerable version of SCP.

Suggestions:

If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056.
HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.
Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates.
You can confirm if this vulnerability is present on your computer as follows.
On a Unix prompt, type these commands:
a. touch foo bar
b. mkdir "any_directory"
c. scp foo bar "any_directory"
If the output is:
"cp: cannot stat `foo': No such file or directory
cp: cannot stat `bar': No such file or directory"
then your OpenSSH is vulnerable. Refer to the following link for Redhat advisoryRHSA-2006:0044-14.
Refer to Vmware advisoryVMware Patch 9986131,
yVMware Patch 3069097.

OpenSSH < 5.2/5.2p1

Impact: Level 2 - Medium

CVSS Score: 1.2

CVE Reference: CVE-2008-3259

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95122
Bugtraq ID: 30339
CVE ID: 2008-3259
FrSIRT Advisory: ADV-2008-2148
ISS X-Force ID: 43940
Secunia Advisory ID: 31179
Security Tracker: 1020537

192.168.235.51 : Potential Vulnerabilities

Vendor Specific News/Changelog Entry: http://openssh.com/security.html
Vendor Specific News/Changelog Entry: http://www.openssh.com/txt/release-5.1

Issue Description:

OpenSSH version is older than 5.2/5.2p1.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.2, is below:
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

OpenSSH GSSAPI Credential Disclosure Vulnerability

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: CVE-2005-2798

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 19592
http://www.mindrot.org/pipermail/openssh-unix-announce/2005-September/000083.html

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host may allow GSSAPI credentials to be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled.

Suggestions:

Upgrade to OpenSSH 4.2 or later.

192.168.235.52 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
3Com 8760
PORT - Port/Protocol/Service/Banner Information
443/tcp(www) none
PORT - Port/Protocol/Service/Banner Information
2313/tcp(unknown) none
PORT - Port/Protocol/Service/Banner Information
22/tcp(ssh) SSH-2.0-SSH_0.2
PORT - Port/Protocol/Service/Banner Information
23/tcp(telnet) Username:
PORT - Port/Protocol/Service/Banner Information
80/tcp(www) none

Open Ports

Port	Protocol	Service	Comment
22	tcp	ssh	Banner - SSH-2.0-SSH_0.2
23	tcp	telnet	Banner - Username:
80	tcp	http	Banner - 3Com Wireless 8760 Dual Radio 11a/b/g Access Point
161	udp	snmp	Service - SNMP
443	tcp	https	Service - OpenSSL
1025	udp	blackjack	Service - blackjack
2313	tcp	iapp	Unknown
7000	udp	afs3-fileserver	Service - afs3-fileserver

192.168.235.52 : Vulnerabilities

SNMP Weak / Guessable Community String

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-2001-0514, CVE-2002-0109, CVE-2004-0311, CVE-2004-1473, CVE-2004-1474

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10264
Bugtraq ID: 11237, 2112, 9681, 6825, 177, 10576, 7081, 7212, 7317, 986
CERT VU: 329230
CVE ID: 1999-0517, 2004-0311, 1999-0254, 1999-0516, 1999-0186, 2004-1473
Generic Exploit URL: http://packetstormsecurity.nl/0402-exploits/apc_9606_backdoor.txt
Generic Informational URL: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Guessable_Read_Community.html&fact_color=doc&tag=
Generic Informational URL: http://www.securiteam.com/exploits/Patrol_s_SNMP_Agent_3_2_can_lead_to_root_compromise.html
Generic Informational URL: http://www.securiteam.com/exploits/Windows_NT_s_SNMP_service_vulnerability.html
ISS X-Force ID: 1240, 15238, 1387, 1241, 1385, 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0460.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0517.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0527.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Microsoft Knowledge Base Article: 99880
Other Advisory URL: http://cert.uni-stuttgart.de/archive/bugtraq/1998/11/msg00249.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/advise12
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 10905, 12635
Security Tracker: 1011388, 1011389
Snort Signature ID: 1411, 1412, 1413, 1414, 1892, 1893, 2406
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-22-00178-1&searchclause=00178
Vendor Specific Advisory URL: http://www.auscert.org.au/render.html?it=494
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1582
Vendor Specific Solution URL: http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch
Vendor Specific Solution URL: http://www.sun.com/solstice/products/ent.agents/

192.168.235.52 : Vulnerabilities

Vendor URL: http://www.apcc.com/
Vendor URL: http://www.managementsoftware.hp.com/
Vendor URL: http://www.symantec.com/

Issue Description:

The SNMP community string on the remote host is still set to the default or can easily be guessed.

Simple Network Management Protocol (SNMP) is used to remotely manage or monitor a host or network device. If an attacker is able to guess the read community string, an attacker will be able to freely view information like the operating system version, IP addresses, interfaces, processes/services, usernames, shares, etc. If the write community string is guessable an attacker has the ability to change system information, leading to anything from a partial to full compromise of the remote host.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community
strings :
- public

Suggestions:

SNMP should preferably be removed if not in use.;;
Alternatively, the following security precautions should be put in place:;
- All community strings should be set to stronger, less easily guessable alternatives.;
- If SNMP is only used for monitoring purposes, write access should be disabled.;
- SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).;
- Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;;
For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:;
Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;

SSL 2.0 Protocol Usage

Impact: Level 5 - Urgent

CVSS Score: 5

CVE Reference: CVE-2005-2969

Port/Protocol: 443/TCP

Other References:

192.168.235.52 : Vulnerabilities

Nessus NASL ID : 20007
http://www.schneier.com/paper-ssl.pdf
http://secunia.com/advisories/17151/
http://www.securiteam.com/securitynews/6Y00D0AEBW.html
http://devedge-temp.mozilla.org/viewsource/2001/tls-ssl3/
http://support.microsoft.com/kb/187498

Issue Description:

The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

The vulnerability is caused due to an error in handling the use of "SSL_OP_MSIE_SSLV2_RSA_PADDING" option. The use of this option causes a verification check that prevents protocol-version rollback attacks to be disabled. This may be exploited in "man-in-the-middle" attacks to force a client and a server to negotiate the less secure SSL 2.0 protocol even when both parties support the more secure SSL 3.0 or TLS 1.0 protocols. The option is also enabled when the "SSL_OP_ALL" option is used.
Successful exploitation requires that SSL 2.0 is enabled, and either the "SSL_OP_MSIE_SSLV2_RSA_PADDING" or the "SSL_OP_ALL" option is used.

Suggestions:

Make sure to disable the SSL 2.0 protocol
OpenSSL 0.9.7 branch:
Update to version 0.9.7h or later.
OpenSSL 0.9.8 branch:
Update to version 0.9.8a or later.
IIS:
http://support.microsoft.com/kb/187498 or
http://support.microsoft.com/kb/245030/

Writeable SNMP Information

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0792, CVE-2000-0147, CVE-2001-0380, CVE-2001-1210, CVE-2002-0478, CVE-2000-0515

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 95160

192.168.235.52 : Vulnerabilities

Bugtraq ID: 973, 1327, 3758, 4330

Issue Description:

Unauthorized users can modify all SNMP information because the access password is not secure.

The system can be attacked in a number of ways--by route redirection, denial of service, complete loss of network service, reboots or crashes, and traffic monitoring.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community
strings :
- private

Suggestions:

If SNMP access is not required on this system, then disallow it. Otherwise, use a secure un-guessable "community name", and restrict the hosts that talk SNMP with your system to a defined list of IP addresses.

Multiple Vendor Malformed SNMP Trap Handling DoS

Impact: Level 4 - Critical

CVE Reference: CVE-2002-0013, CVE-2002-0012

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10858

Issue Description:

It was possible to disable the remote SNMP daemon by sending
a malformed packet advertising bogus length fields.
An attacker may use this flaw to prevent you from using
SNMP to administer your network (or use other flaws
to execute arbitrary code with the privileges of the
SNMP daemon).
Solution :
See www.cert.org/advisories/CA-2002-03.html
Risk factor : High

Suggestions:

192.168.235.52 : Vulnerabilities

See www.cert.org/advisories/CA-2002-03.html

3Com Wireless Access Point Default Password Vulnerability

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95218

Issue Description:

The user name and password for the administration panel of the wireless access point are set to the manufacturer's default values, allowing unauthorized users to change the configuration of the wireless access point.

By exploiting this vulnerability, users may be able to inspect and change the configuration of the wireless access point. Users in close proximity to the wireless access point (typically up to 1500 feet) may also be able to exploit this issue. By lowering the security settings of the wireless access point, a malicious user may be able to communicate with other computers on the network, which may lead to further attacks.

Raw Scanner Output:

Username: admin
Password: password

Suggestions:

Configure a user name and password that are difficult for a malicious user to guess.

3Com Wireless Access Point Default Password Vulnerability

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

192.168.235.52 : Vulnerabilities

Nessus NASL ID : 95218

Issue Description:

The user name and password for the administration panel of the wireless access point are set to the manufacturer's default values, allowing unauthorized users to change the configuration of the wireless access point.

By exploiting this vulnerability, users may be able to inspect and change the configuration of the wireless access point. Users in close proximity to the wireless access point (typically up to 1500 feet) may also be able to exploit this issue. By lowering the security settings of the wireless access point, a malicious user may be able to communicate with other computers on the network, which may lead to further attacks.

Raw Scanner Output:

Username: admin
Password: password

Suggestions:

Configure a user name and password that are difficult for a malicious user to guess.

SSL Medium Strength Cipher Suites Supported

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42873

Issue Description:

The remote service supports the use of medium strength SSL ciphers.

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Raw Scanner Output:

Plugin output :
Here are the medium strength SSL ciphers supported by the remote server :
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)

192.168.235.52 : Vulnerabilities

```
   SSLv2
     DES-CBC-MD5              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=MD5
     RC4-64-MD5               Kx=RSA       Au=RSA     Enc=RC4(64)
Mac=MD5
   SSLv3
     DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
   TLSv1
     EXP1024-DES-CBC-SHA      Kx=RSA(1024)  Au=RSA     Enc=DES(56)
Mac=SHA1   export
     EXP1024-RC2-CBC-MD5      Kx=RSA(1024)  Au=RSA     Enc=RC2(56)
Mac=MD5    export
     EXP1024-RC4-MD5          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=MD5    export
     EXP1024-RC4-SHA          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=SHA1   export
     DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
The fields above are :
 {OpenSSL ciphername}
 Kx={key exchange}
 Au={authentication}
 Enc={symmetric encryption method}
 Mac={message authentication code}
 {export flag}
```

Suggestions:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Weak Supported SSL Ciphers Suites

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 26928
The following links detail how to change the supported SSL Cipher Suites for IIS:;;
How to control the ciphers for SSL and TLS;
----------;
http://support.microsoft.com/kb/216482;;
How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll;

192.168.235.52 : Vulnerabilities

---;
http://support.microsoft.com/kb/245030;;
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services;
---;
http://support.microsoft.com/kb/187498;;
Apache;
---;
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite;;
IBM HTTP Server;
---;
ftp://ftp.software.ibm.com/software/webserver/appserv/library/v60/ihs_60.pdf;;
iPlanet;
---;
http://docs.sun.com/source/816-5682-10/esecurty.htm#1008479;;
Note: It must be noted that these changes have not been tested by
SensePost, so the impact of these changes is unknown. The possibility exists that older Internet Browsing software may not be able to access the SSL protected portions of these websites, should they not have support for certain ciphers.;

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Weaker cyphers have a higher possibility of being cracked and as such it is recommended that 128bit cyphers be used, at a minimum.

Raw Scanner Output:

Plugin output :
Here is the list of weak SSL ciphers supported by the remote server :
  Low Strength Ciphers (< 56-bit key)
    SSLv2
      EXP-RC2-CBC-MD5   Kx=RSA(512)   Au=RSA   Enc=RC2(40)
Mac=MD5   export
      EXP-RC4-MD5   Kx=RSA(512)   Au=RSA   Enc=RC4(40)
Mac=MD5   export
    SSLv3
      EXP-DES-CBC-SHA   Kx=RSA(512)   Au=RSA   Enc=DES(40)
Mac=SHA1   export
      EXP-RC2-CBC-MD5   Kx=RSA(512)   Au=RSA   Enc=RC2(40)
Mac=MD5   export
      EXP-RC4-MD5   Kx=RSA(512)   Au=RSA   Enc=RC4(40)
Mac=MD5   export
    TLSv1
      EXP-DES-CBC-SHA   Kx=RSA(512)   Au=RSA   Enc=DES(40)
Mac=SHA1   export
      EXP-RC2-CBC-MD5   Kx=RSA(512)   Au=RSA   Enc=RC2(40)
Mac=MD5   export
      EXP-RC4-MD5   Kx=RSA(512)   Au=RSA   Enc=RC4(40)

192.168.235.52 : Vulnerabilities

Mac=MD5 export
The fields above are :
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

Web Server Uses Plain Text Authentication Forms

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 26194

Issue Description:

The remote web server contains a HTML form containing an input of type "password" which transmits possibly sensitive information in plain text.

Raw Scanner Output:

Plugin output :
Page : /
Destination page : index.htm
Input name : passwd
Page : /index.htm?userid=&passwd=&Submit=LOGIN&Close=CANCEL
Destination page : index.htm
Input name : passwd

Suggestions:

Ensure that all sensitive information is transmitted to the remote webserver securely. SSL is the most common means of providing this security.

Unencrypted Telnet Server

192.168.235.52 : Vulnerabilities

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 42263

Issue Description:

The remote Telnet server transmits traffic in cleartext.

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Suggestions:

Disable this service and use SSH instead.

Comments:

Created On: 2009-12-22 12:50:57
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across open networks such as the Internet.

SSL Certificate - Signature Verification Failed Vulnerability

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95242

Issue Description:

192.168.235.52 : Vulnerabilities

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Impact: Level 2 - Medium

CVSS Score: 6.4

CVE Reference: CVE-2009-3555

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42880
http://extendedsubset.com/?p=8
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.kb.cert.org/vuls/id/120541
http://www.g-sec.lu/practicaltls.pdf
https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt
BID:36935
OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974

Issue Description:

The remote service allows renegotiation of TLS / SSL connections.

Suggestions:

No suggestion at this time

192.168.235.52 : Vulnerabilities

Web Server Allows Password Auto-Completion

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 42057

Issue Description:

Auto-complete is not disabled on password fields.

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Raw Scanner Output:

Plugin output :
Page : /
Destination Page : index.htm
Input name : passwd
Page : /index.htm?userid=&passwd=&Submit=LOGIN&Close=CANCEL
Destination Page : index.htm
Input name : passwd

Suggestions:

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

CN does not match hostname

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

192.168.235.52 : Vulnerabilities

Nessus NASL ID : 95137

Telnet Service and Version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 10281

Issue Description:

This detects the Telnet server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and types should be omitted where possible.

Raw Scanner Output:

Plugin output :
Here is the banner from the remote Telnet server :
---------- snip ----------
Username:
---------- snip ----------

Suggestions:

Informational plugin.

Self-signed certificate

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

192.168.235.52 : Vulnerabilities

Nessus NASL ID : 95138

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers. By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

Web Server Allows Password Auto-Completion

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 42057

Issue Description:

Auto-complete is not disabled on password fields.

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Raw Scanner Output:

Plugin output :
Page : /
Destination Page : index.htm

192.168.235.52 : Vulnerabilities

Input name : passwd
Page : /index.htm?userid=&passwd=&Submit=LOGIN&Close=CANCEL
Destination Page : index.htm
Input name : passwd

Suggestions:

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
Pragma: no-cache
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the

192.168.235.52 : Vulnerabilities

web server configuration file.

SSL Certificate Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10863

Issue Description:

The scanner was able to determine what SSL ciphers are supported by the server.

The use of weak ciphers may lead to the compromise of data in transit.

Raw Scanner Output:

Plugin output :
Subject Name:
Country: US
State/Province: Massachusetts
Locality: Marlborough
Organization: 3Com Corporation
Organization Unit: Wireless
Common Name: 3Com Wireless LAN Access Point
Email Address: support.3com.com
Issuer Name:
Country: US
State/Province: Massachusetts
Locality: Marlborough
Organization: 3Com Corporation
Organization Unit: Wireless
Common Name: 3Com Wireless LAN Access Point
Email Address: support.3com.com
Serial Number: 00
Version: 1
Signature Algorithm: SHA-1 With RSA Encryption
Not Valid Before: Jan 21 05:35:41 2005 GMT
Not Valid After: Jan 21 05:35:41 2025 GMT
Public Key Info:
Algorithm: RSA Encryption
Public Key: 00 AE 62 86 99 4F 00 F7 9C 10 BD 9C CD 53 0A F6 24 0F 63 90

192.168.235.52 : Vulnerabilities

02 AE 0D 47 4E BF 68 68 45 72 62 AA 66 66 59 E0 00 A5 D5 ED
87 55 3F 98 B6 70 B8 D0 44 F2 86 23 1A 4F 24 DD AB 0B 04 3A
07 AC 53 13 07 5A 32 78 65 6F F9 5D 9F B5 0E D7 FD C4 BA E0
81 EB D9 A4 B1 CB 28 BE 2D 29 EE 11 F9 81 F7 D2 90 00 86 8C
93 DA 3E 7D 3E CA E6 7A 2C A5 79 12 F6 93 79 C2 CC 8F D8 E8
8F 84 55 96 2C BD 32 2E 00 44 DB 57 06 E8 3E CF 36 02 76 09
85 4F 24 61 F6 8C 88 0C B8 AF 76 67 48 7B 65 12 D9 42 64 0E
96 48 D9 C6 2F 3D 30 16 2B 82 15 BB 94 96 49 D5 64 58 4E 29
65 C0 EF 54 82 34 D9 CB B9 BA CA EB 1C A5 6F DD EF 73 14 D1
6D CD FB 5D 84 85 FC D6 20 B1 AB 22 19 C6 AB 92 40 8A BF BC
98 33 BC 40 CF E4 CD 47 22 0B 74 1D 8C 74 AB CD AB 52 14 81
BE E8 75 1E 18 11 B3 61 6D B3 E5 A6 AD 03 78 DF B7

Exponent: 01 00 01

Signature: 00 00 4F 20 A3 08 19 DC 5F 25 76 F0 56 82 84 A4 ED AD 60 06
64 4D 66 8A 20 59 3D CA ED FD 7B F6 1B 53 26 1D DE 2E 99 D8
80 AE B0 AA 9F 32 4E 54 05 19 EF 70 42 58 96 44 B8 5B A0 8F
CB 9F 6C B5 8B C4 AE D4 DF A2 43 EC BF C3 85 8E 99 08 2E D5
50 84 BA BF 47 51 B5 BB 48 89 90 EB 42 3A 3E 64 7C 7F 87 D0
4B 8F 30 7B E8 42 E4 73 A8 16 87 FA 69 AE 28 F1 A2 3B BB 91
3B 5D F8 4D 72 9D 0E C8 A7 C2 05 99 EF 20 C7 06 19 6C 1A 62
23 55 5A DE 1A F9 30 DB 67 20 F8 B7 3D 31 A4 7D 99 51 31 23
E3 7C 8B 71 F5 E2 BD 70 1B 3E 01 3B 46 3E 26 D2 85 18 F9 0A
AA EC 36 F1 25 AB 23 C0 DA DB 57 A1 DD 48 F2 65 AC 3E F4 E4
F6 FD C6 53 BC 52 CB 42 7A 44 18 71 E9 3D C4 2F CC AC 86 AA
BB 3C 33 CD A9 10 3D 89 26 AD C7 23 D0 54 B5 9F BC 94 56 67
63 2D AE 8A E8 C6 1D E0 E1 77 46 C8 49 69 0D E7 AD

Suggestions:

Informational plugin.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

192.168.235.52 : Vulnerabilities

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : VxWorks
Confidence Level : 65
Method : SinFP
The remote host is running VxWorks

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSLv2 server answered on this port.

Suggestions:

Informational plugin.

ICMP timestamp request

Impact: Level 1 - Low

192.168.235.52 : Vulnerabilities

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The difference between the local and remote clocks is 78559 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and

192.168.235.52 : Vulnerabilities

whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

Supported SSL Ciphers Suites

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

192.168.235.52 : Vulnerabilities

Other References:

Nessus NASL ID : 21643
http://www.openssl.org/docs/apps/ciphers.html

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Raw Scanner Output:

```
Plugin output :
Here is the list of SSL ciphers supported by the remote server :
  Low Strength Ciphers (< 56-bit key)
    SSLv2
      EXP-RC2-CBC-MD5           Kx=RSA(512)   Au=RSA     Enc=RC2(40)
Mac=MD5    export
      EXP-RC4-MD5               Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    SSLv3
      EXP-DES-CBC-SHA           Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC2-CBC-MD5           Kx=RSA(512)   Au=RSA     Enc=RC2(40)
Mac=MD5    export
      EXP-RC4-MD5               Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    TLSv1
      EXP-DES-CBC-SHA           Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC2-CBC-MD5           Kx=RSA(512)   Au=RSA     Enc=RC2(40)
Mac=MD5    export
      EXP-RC4-MD5               Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv2
      DES-CBC-MD5               Kx=RSA        Au=RSA     Enc=DES(56)
Mac=MD5
      RC4-64-MD5                Kx=RSA        Au=RSA     Enc=RC4(64)
Mac=MD5
    SSLv3
      DES-CBC-SHA               Kx=RSA        Au=RSA     Enc=DES(56)
Mac=SHA1
    TLSv1
      EXP1024-DES-CBC-SHA       Kx=RSA(1024)  Au=RSA     Enc=DES(56)
Mac=SHA1   export
      EXP1024-RC2-CBC-MD5       Kx=RSA(1024)  Au=RSA     Enc=RC2(56)
Mac=MD5    export
```

192.168.235.52 : Vulnerabilities

```
    EXP1024-RC4-MD5          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=MD5    export
    EXP1024-RC4-SHA          Kx=RSA(1024)  Au=RSA     Enc=RC4(56)
Mac=SHA1   export
    DES-CBC-SHA              Kx=RSA        Au=RSA     Enc=DES(56)
Mac=SHA1
  High Strength Ciphers (>= 112-bit key)
   SSLv2
    IDEA-CBC-MD5             Kx=RSA        Au=RSA     Enc=IDEA(128)
Mac=MD5
    RC2-CBC-MD5              Kx=RSA        Au=RSA     Enc=RC2(128)
Mac=MD5
    RC4-MD5                  Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
   SSLv3
    DES-CBC3-SHA             Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
    IDEA-CBC-SHA             Kx=RSA        Au=RSA     Enc=IDEA(128)
Mac=SHA1
    RC4-MD5                  Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
    RC4-SHA                  Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1
   TLSv1
    DES-CBC3-SHA             Kx=RSA        Au=RSA     Enc=3DES(168)
Mac=SHA1
    IDEA-CBC-SHA             Kx=RSA        Au=RSA     Enc=IDEA(128)
Mac=SHA1
    RC4-MD5                  Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=MD5
    RC4-SHA                  Kx=RSA        Au=RSA     Enc=RC4(128)
Mac=SHA1
The fields above are :
 {OpenSSL ciphername}
 Kx={key exchange}
 Au={authentication}
 Enc={symmetric encryption method}
 Mac={message authentication code}
 {export flag}
```

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

CGI's Found

Impact: Level 1 - Low

192.168.235.52 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 10662

Issue Description:

This script makes a mirror of the remote web site(s)and extracts the list of CGIs that are used by the remote host. Please refer to 'details' for more information.

Raw Scanner Output:

Plugin output :
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/index.htm (Close [CANCEL] passwd [] Submit [LOGIN] userid [])

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port through SSLv2.

192.168.235.52 : Vulnerabilities

Suggestions:

Informational plugin.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-2.0-SSH_0.2
SSH supported authentication : password

Suggestions:

Informational plugin.

CGI's Found

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

192.168.235.52 : Vulnerabilities

Nessus NASL ID : 10662

Issue Description:

This script makes a mirror of the remote web site(s)and extracts the list of CGIs that are used by the remote host. Please refer to 'details' for more information.

Raw Scanner Output:

Plugin output :
The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/index.htm (Close [CANCEL] passwd [] Submit [LOGIN] userid [])

Suggestions:

Informational plugin.

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

192.168.235.52 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.52 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.187.74
4.68.110.77
4.68.16.190
4.69.134.121
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.52

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

Service detection

Impact: Level 1 - Low

192.168.235.52 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A telnet server is running on this port.

Suggestions:

Informational plugin.

192.168.235.54 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
db5
OS - OS Name
Windows 5.2
PORT - Port/Protocol/Service/Banner Information
445/tcp(cifs) none
PORT - Port/Protocol/Service/Banner Information
5560/tcp(www) Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
PORT - Port/Protocol/Service/Banner Information
5580/tcp(oracle_application_server) none
PORT - Port/Protocol/Service/Banner Information
20034/tcp(unknown) none
PORT - Port/Protocol/Service/Banner Information
1521/tcp(oracle_tnslsnr) none
PORT - Port/Protocol/Service/Banner Information
1158/tcp(www) Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
PORT - Port/Protocol/Service/Banner Information
5520/tcp(oracle_application_server) none
PORT - Port/Protocol/Service/Banner Information
3938/tcp(www) none
PORT - Port/Protocol/Service/Banner Information
135/tcp(DCE) e1af82308-5d1f-11c9-51a4-08002b14a0fa none
PORT - Port/Protocol/Service/Banner Information
139/tcp(smb) none

Open Ports

Port	Protocol	Service	Comment
123	udp	ntp	Service - NTP
135	tcp	epmap	Service - Microsoft Windows RPC
137	udp	netbios-ns	Service - netbios-ns
138	udp	netbios-dgm	Service - netbios-dgm
139	tcp	netbios-ssn	Service - netbios-ssn
445	udp	microsoft-ds	Service - microsoft-ds
445	tcp	microsoft-ds	Service - microsoft-ds
500	udp	isakmp	Service - isakmp
1158	tcp	unknown	Banner - Oracle Application Server httpd 9.0.4.1.0
1521	tcp	ncube-lm	Banner - Oracle TNS Listener" version="10.2.0.1.0 (for 32-bit Windows)
3938	tcp	unknown	Service - Oracle Enterprise Management Agent httpd
5520	tcp	sdlog	Service - Oracle Enterprise Manager
5560	tcp	unknown	Banner - Server: Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
5580	tcp	unknown	Service - Oracle Enterprise Manager
20034	tcp	netbus-pro	Unkown

192.168.235.54 : Vulnerabilities

SMB Login

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0504, CVE-1999-0506, CVE-2000-0222, CVE-1999-0505, CVE-2002-1117, CVE-1999-0503, CVE-2005-3595

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10394
BID: 494, 990, 11199
Microsoft:
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP
CVE ID: 2002-1117
Generic Informational URL: http://www.sans.org/top20/oct02.php#W1
ISS X-Force ID: 10093, 17412
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0170.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0203.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0607.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0623.html
Mail List Post: http://archives.neohapsis.com/archives/vulndiscuss/2004-q3/0019.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00235.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00364.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Microsoft Knowledge Base Article: 143474
Microsoft Knowledge Base Article: 246261
Security Tracker: 1011344
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
Vendor URL: http://www.ibm.com/us/
Vendor URL: http://www.microsoft.com/

Issue Description:

This plugin attempts to log into the remote host using several username/password combinations. This however includes Null / Anonymous connections.

Raw Scanner Output:

Plugin output :
- NULL sessions are enabled on the remote host

192.168.235.54 : Vulnerabilities

Suggestions:

To fix this issue, edit the following key :
HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2.
Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.

Oracle Default Accounts

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 22075
http://www.petefinnigan.com/

Issue Description:

The remote host is an Oracle Database server. Older versions of this server used to come bundled with several default accounts.

An attacker may use these accounts to get access to the remote database and read and temper its data.

Raw Scanner Output:

Synopsis :
One or more default accounts have been found in the remote database.
Description :
The remote host is an Oracle Database server. Older versions of this
server and versions included in third-party software are bundled with
several default accounts.
An attacker may use these accounts to get access to the remote
database and read and modify its data.
See also :
http://www.petefinnigan.com/
http://archives.neohapsis.com/archives/bugtraq/2009-10/0142.html
Solution :
If using a third-party product, contact the vendor for an update.
Otherwise, either disable the reported accounts or change the
associated passwords.
Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
Plugin output :

192.168.235.54 : Vulnerabilities

The following default accounts have been found :

Account : BRIO_ADMIN, password : BRIO_ADMIN
Account : BRUGERNAVN, password : ADGANGSKODE
Account : BRUKERNAVN, password : PASSWORD
Account : BSC, password : BSC
Account : BUG_REPORTS, password : BUG_REPORTS
Account : CALVIN, password : HOBBES
Account : CATALOG, password : CATALOG
Account : CCT, password : CCT
Account : CDEMO82, password : CDEMO82
Account : CDEMO82, password : CDEMO83
Account : CDEMO82, password : UNKNOWN
Account : CDEMOCOR, password : CDEMOCOR
Account : CDEMORID, password : CDEMORID
Account : CDEMOUCB, password : CDEMOUCB
Account : CDOUGLAS, password : CDOUGLAS
Account : CE, password : CE
Account : CENTRA, password : CENTRA
Account : CENTRAL, password : CENTRAL
Account : CIDS, password : CIDS
Account : CIS, password : CIS
Account : CIS, password : ZWERG
Account : CISINFO, password : CISINFO
Account : CISINFO, password : ZWERG
Account : CLARK, password : CLOTH
Account : CN, password : CN
Account : COMPANY, password : COMPANY
Account : COMPIERE, password : COMPIERE
Account : CQSCHEMAUSER, password : PASSWORD
Account : CQUSERDBUSER, password : PASSWORD
Account : CRP, password : CRP
Account : CS, password : CS
Account : CSC, password : CSC
Account : CSD, password : CSD
Account : CSE, password : CSE
Account : CSF, password : CSF
Account : CSI, password : CSI
Account : CSL, password : CSL
Account : CSMIG, password : CSMIG
Account : CSP, password : CSP
Account : CSR, password : CSR
Account : CSS, password : CSS
Account : CTXDEMO, password : CTXDEMO
Account : CTXSYS, password : CHANGE_ON_INSTALL
Account : CTXSYS, password : CTXSYS
Account : CTXSYS, password : UNKNOWN
Account : CUA, password : CUA
Account : CUE, password : CUE
Account : CUF, password : CUF
Account : CUG, password : CUG

192.168.235.54 : Vulnerabilities

Account : CUI, password : CUI
Account : CUN, password : CUN
Account : CUP, password : CUP
Account : CUS, password : CUS
Account : CZ, password : CZ
Account : DBI, password : MUMBLEFRATZ
Account : HR, password : CHANGE_ON_INSTALL
Account : HR, password : HR
Account : HRI, password : HRI
Account : HVST, password : HVST
Account : HXC, password : HXC
Account : HXT, password : HXT
Account : IBA, password : IBA
Account : IBE, password : IBE
Account : IBP, password : IBP
Account : IBU, password : IBU
Account : IBY, password : IBY
Account : ICDBOWN, password : ICDBOWN
Account : ICX, password : ICX
Account : IDEMO_USER, password : IDEMO_USER
Account : IEB, password : IEB
Account : IEC, password : IEC
Account : IEM, password : IEM
Account : IEO, password : IEO
Account : IES, password : IES
Account : IEU, password : IEU
Account : IEX, password : IEX
Account : IFSSYS, password : IFSSYS
Account : IGC, password : IGC
Account : IGF, password : IGF
Account : IGI, password : IGI
Account : IGS, password : IGS
Account : IGW, password : IGW
Account : IMAGEUSER, password : IMAGEUSER
Account : IMC, password : IMC
Account : IMEDIA, password : IMEDIA
Account : IMT, password : IMT
Account : #INTERNAL, password : ORACLE
Account : #INTERNAL, password : SYS_STNT
Account : INV, password : INV
Account : IPA, password : IPA
Account : IPD, password : IPD
Account : IPLANET, password : IPLANET
Account : ISC, password : ISC
Account : ITG, password : ITG
Account : JA, password : JA
Account : JAKE, password : PASSWO4
Account : JE, password : JE
Account : JG, password : JG
Account : JILL, password : PASSWO2

192.168.235.54 : Vulnerabilities

Account : JL , password : JL
Account : JMUSER, password : JMUSER
Account : JOHN, password : JOHN
Account : JONES, password : STEEL
Account : JTF, password : JTF
Account : JTM, password : JTM
Account : JTS, password : JTS
Account : JWARD, password : AIROPLANE
Account : KWALKER, password : KWALKER
Account : L2LDEMO, password : L2LDEMO
Account : LBACSYS, password : LBACSYS
Account : LIBRARIAN, password : SHELVES
Account : MANPROD, password : MANPROD
Account : MARK, password : PASSWO3
Account : MASCARM, password : MANAGER
Account : MASTER, password : PASSWORD
Account : MDDATA, password : MDDATA
Account : MDDEMO, password : MDDEMO
Account : MDDEMO_CLERK, password : CLERK
Account : MDDEMO_CLERK, password : MGR
Account : MDDEMO_MGR, password : MDDEMO_MGR
Account : MDSYS, password : MDSYS
Account : ME, password : ME
Account : MFG, password : MFG
Account : MGR, password : MGR
Account : MGWUSER, password : MGWUSER
Account : MIGRATE, password : MIGRATE
Account : MILLER, password : MILLER
Account : MMO2, password : MMO2
Account : MMO2, password : MMO3
Account : MMO2, password : UNKNOWN
Account : MODTEST, password : YES
Account : MOREAU, password : MOREAU
Account : MRP, password : MRP
Account : MSC, password : MSC
Account : MSD, password : MSD
Account : MSO, password : MSO
Account : MSR, password : MSR
Account : MTS_USER, password : MTS_PASSWORD
Account : MTSSYS, password : MTSSYS
Account : MWA, password : MWA
Account : MXAGENT, password : MXAGENT
Account : NAMES, password : NAMES
Account : NEOTIX_SYS, password : NEOTIX_SYS
Account : NNEUL, password : NNEULPASS
Account : NOM_UTILISATEUR, password : MOT_DE_PASSE
Account : NOMEUTENTE, password : PASSWORD
Account : NOME_UTILIZADOR, password : SENHA
Account : NUME_UTILIZATOR, password : PAROL
Account : OAS_PUBLIC, password : OAS_PUBLIC

192.168.235.54 : Vulnerabilities

Account : OCITEST, password : OCITEST
Account : OCM_DB_ADMIN, password : OCM_DB_ADMIN
Account : ODM, password : ODM
Account : ODM_MTR, password : MTRPW
Account : ODS, password : ODS
Account : ODS_SERVER, password : ODS_SERVER
Account : ODSCOMMON, password : ODSCOMMON
Account : OE, password : CHANGE_ON_INSTALL
Account : OE, password : UNKNOWN
Account : OE, password : OE
Account : OEMADM, password : OEMADM
Account : OEMREP, password : OEMREP
Account : OKB, password : OKB
Account : OKC, password : OKC
Account : OKE, password : OKE
Account : OKI, password : OKI
Account : OKO, password : OKO
Account : OKR, password : OKR
Account : OKS, password : OKS
Account : OKX, password : OKX
Account : OLAPDBA, password : OLAPDBA
Account : OLAPSVR, password : INSTANCE
Account : OLAPSVR, password : OLAPSVR
Account : OLAPSYS, password : MANAGER
Account : OLAPSYS, password : OLAPSYS
Account : OMWB_EMULATION, password : ORACLE
Account : ONT, password : ONT
Account : OO, password : OO
Account : OPENSPIRIT, password : OPENSPIRIT
Account : OPI, password : OPI
Account : ORACACHE, password : ORACACHE
Account : ORACLE, password : ORACLE
Account : ORADBA, password : ORADBAPASS
Account : ORAPROBE, password : ORAPROBE
Account : ORAREGSYS, password : ORAREGSYS
Account : ORASSO, password : ORASSO
Account : ORASSO_DS, password : ORASSO_DS
Account : ORASSO_PA, password : ORASSO_PA
Account : ORASSO_PS, password : ORASSO_PS
Account : ORASSO_PUBLIC, password : ORASSO_PUBLIC
Account : ORASTAT, password : ORASTAT
Account : ORCLADMIN, password : WELCOME
Account : ORDCOMMON, password : ORDCOMMON
Account : DATA_SCHEMA, password : LASKJDF098KSDAF09
Account : DBSNMP, password : DBSNMP
Account : DBVISION, password : DBVISION
Account : DDIC, password : 199220706
Account : DEMO, password : DEMO
Account : DEMO8, password : DEMO8
Account : DEMO9, password : DEMO9

192.168.235.54 : Vulnerabilities

Account : DES, password : DES
Account : DES2K, password : DES2K
Account : DEV2000_DEMOS, password : DEV2000_DEMOS
Account : DIANE, password : PASSWO1
Account : DIP, password : DIP
Account : DISCOVERER_ADMIN, password : DISCOVERER_ADMIN
Account : DMSYS, password : DMSYS
Account : DPF, password : DPFPASS
Account : DSGATEWAY, password : DSGATEWAY
Account : DSSYS, password : DSSYS
Account : DTSP, password : DTSP
Account : EAA, password : EAA
Account : EAM, password : EAM
Account : EARLYWATCH, password : SUPPORT
Account : EAST, password : EAST
Account : EC, password : EC
Account : ECX, password : ECX
Account : EJB, password : EJB
Account : EJSADMIN, password : EJSADMIN
Account : EJSADMIN, password : EJSADMIN_PASSWORD
Account : EMP, password : EMP
Account : ENG, password : ENG
Account : ENI, password : ENI
Account : ESTOREUSER, password : ESTORE
Account : EVENT, password : EVENT
Account : EVM, password : EVM
Account : EXAMPLE, password : EXAMPLE
Account : EXFSYS, password : EXFSYS
Account : EXTDEMO, password : EXTDEMO
Account : EXTDEMO2, password : EXTDEMO2
Account : FA, password : FA
Account : FEM, password : FEM
Account : FII, password : FII
Account : FINANCE, password : FINANCE
Account : FINPROD, password : FINPROD
Account : FLM, password : FLM
Account : FND, password : FND
Account : FOO, password : BAR
Account : FPT, password : FPT
Account : FRM, password : FRM
Account : FROSTY, password : SNOWMAN
Account : FTE, password : FTE
Account : FV, password : FV
Account : GL, password : GL
Account : GMA, password : GMA
Account : GMD, password : GMD
Account : GME, password : GME
Account : GMF, password : GMF
Account : GMI, password : GMI
Account : GML, password : GML

192.168.235.54 : Vulnerabilities

Account : GMP, password : GMP
Account : GMS, password : GMS
Account : GPFD, password : GPFD
Account : GPLD, password : GPLD
Account : GR, password : GR
Account : HADES, password : HADES
Account : HCPARK, password : HCPARK
Account : HLW, password : HLW
Account : HR, password : UNKNOWN
Account : ABM, password : ABM
Account : ADAMS, password : WOOD
Account : ADLDEMO, password : ADLDEMO
Account : ADMIN, password : JETSPEED
Account : ADMIN, password : WELCOME
Account : ADMINISTRATOR, password : ADMIN
Account : ADMINISTRATOR, password : ADMINISTRATOR
Account : AHL, password : AHL
Account : AHM, password : AHM
Account : AK, password : AK
Account : ALHRO, password : XXX
Account : ALHRW, password : XXX
Account : ALR, password : ALR
Account : AMS, password : AMS
Account : AMV, password : AMV
Account : ANDY, password : SWORDFISH
Account : AP, password : AP
Account : APPLMGR, password : APPLMGR
Account : APPLSYS, password : APPLSYS
Account : APPLSYS, password : APPS
Account : APPLSYS, password : FND
Account : APPLSYSPUB, password : APPLSYSPUB
Account : APPLSYSPUB, password : PUB
Account : APPLSYSPUB, password : FNDPUB
Account : APPLYSYSPUB, password : FNDPUB
Account : APPLYSYSPUB, password : PUB
Account : APPS, password : APPS
Account : APPS_MRC, password : APPS
Account : APPUSER, password : APPPASSWORD
Account : AQ, password : AQ
Account : AQDEMO, password : AQDEMO
Account : AQJAVA, password : AQJAVA
Account : AQUSER, password : AQUSER
Account : AR, password : AR
Account : ASF, password : ASF
Account : ASG, password : ASG
Account : ASL, password : ASL
Account : ASO, password : ASO
Account : ASP, password : ASP
Account : AST, password : AST
Account : ATM, password : SAMPLEATM

192.168.235.54 : Vulnerabilities

Account : AUDIOUSER, password : AUDIOUSER
Account : AX, password : AX
Account : AZ, password : AZ
Account : BC4J, password : BC4J
Account : BEN, password : BEN
Account : BIC, password : BIC
Account : BIL, password : BIL
Account : BIM, password : BIM
Account : BIS, password : BIS
Account : BIV, password : BIV
Account : BIX, password : BIX
Account : BLAKE, password : PAPER
Account : BLEWIS, password : BLEWIS
Account : BOM, password : BOM
Account : SYSMAN, password : SYSMAN
Account : SYSTEM, password : CHANGE_ON_INSTALL
Account : SYSTEM, password : D_SYSPW
Account : SYSTEM, password : MANAGER
Account : SYSTEM, password : ORACLE
Account : SYSTEM, password : SYSTEMPASS
Account : SYSTEM, password : SYSTEM
Account : SYSTEM, password : MANAG3R
Account : SYSTEM, password : ORACL3
Account : SYSTEM, password : 0RACLE
Account : SYSTEM, password : 0RACL3
Account : SYSTEM, password : ORACLE8
Account : SYSTEM, password : ORACLE9
Account : SYSTEM, password : ORACLE9I
Account : SYSTEM, password : 0RACLE9I
Account : SYSTEM, password : 0RACL39I
Account : TAHITI, password : TAHITI
Account : TALBOT, password : MT6CH5
Account : TDOS_ICSAP, password : TDOS_ICSAP
Account : TEC, password : TECTEC
Account : TEST, password : PASSWD
Account : TEST, password : TEST
Account : TEST_USER, password : TEST_USER
Account : TESTPILOT, password : TESTPILOT
Account : THINSAMPLE, password : THINSAMPLEPW
Account : TIBCO, password : TIBCO
Account : TIP37, password : TIP37
Account : TRACESVR, password : TRACE
Account : TRAVEL, password : TRAVEL
Account : TSDEV, password : TSDEV
Account : TSUSER, password : TSUSER
Account : TURBINE, password : TURBINE
Account : ULTIMATE, password : ULTIMATE
Account : UM_ADMIN, password : UM_ADMIN
Account : UM_CLIENT, password : UM_CLIENT
Account : USER, password : USER

192.168.235.54 : Vulnerabilities

Account : USER_NAME, password : PASSWORD
Account : USER0, password : USER0
Account : USER1, password : USER1
Account : USER2, password : USER2
Account : USER3, password : USER3
Account : USER4, password : USER4
Account : USER5, password : USER5
Account : USER6, password : USER6
Account : USER7, password : USER7
Account : USER8, password : USER8
Account : USER9, password : USER9
Account : UTILITY, password : UTILITY
Account : USUARIO, password : CLAVE
Account : UTLBSTATU, password : UTLESTAT
Account : VEA, password : VEA
Account : VEH, password : VEH
Account : VERTEX_LOGIN, password : VERTEX_LOGIN
Account : VIDEOUSER, password : VIDEOUSER
Account : VIF_DEVELOPER, password : VIF_DEV_PWD
Account : VIRUSER, password : VIRUSER
Account : VPD_ADMIN, password : AKF7D98S2
Account : VRR1, password : VRR1
Account : VRR1, password : VRR2
Account : VRR1, password : UNKNOWN
Account : WEBCAL01, password : WEBCAL01
Account : WEBDB, password : WEBDB
Account : WEBREAD, password : WEBREAD
Account : WEBSYS, password : MANAGER
Account : WEBUSER, password : YOUR_PASS
Account : WEST, password : WEST
Account : WFADMIN, password : WFADMIN
Account : WH, password : WH
Account : WIP, password : WIP
Account : WKADMIN, password : WKADMIN
Account : WKPROXY, password : WKPROXY
Account : WKPROXY, password : CHANGE_ON_INSTALL
Account : WKSYS, password : CHANGE_ON_INSTALL
Account : WKPROXY, password : UNKNOWN
Account : WKSYS, password : WKSYS
Account : WKUSER, password : WKUSER
Account : WK_TEST, password : WK_TEST
Account : WMS, password : WMS
Account : WMSYS, password : WMSYS
Account : WOB, password : WOB
Account : WPS, password : WPS
Account : WSH, password : WSH
Account : WSM, password : WSM
Account : WWW, password : WWW
Account : WWWUSER, password : WWWUSER
Account : XADEMO, password : XADEMO

Account : XDB, password : CHANGE_ON_INSTALL
Account : XDP, password : XDP
Account : XLA, password : XLA
Account : XNC, password : XNC
Account : XNI, password : XNI
Account : XNM, password : XNM
Account : XNP, password : XNP
Account : XNS, password : XNS
Account : XPRT, password : XPRT
Account : XTR, password : XTR
Account : MDDEMO_MGR, password : MGR
Account : SYSTEM, password : D_SYSTPW
Account : SYSTEM, password : ORACLE8I
Account : SYSTEM, password : 0RACLE8
Account : SYSTEM, password : 0RACLE9
Account : SYSTEM, password : 0RACLE8I
Account : SYSTEM, password : 0RACL38
Account : SYSTEM, password : 0RACL39
Account : SYSTEM, password : 0RACL38I
Account : SYS, password : 0RACLE8
Account : SYS, password : 0RACLE9
Account : SYS, password : 0RACLE8I
Account : SYS, password : 0RACL38
Account : SYS, password : 0RACL39
Account : SYS, password : 0RACL38I
Account : ORDPLUGINS, password : ORDPLUGINS
Account : ORDSYS, password : ORDSYS
Account : OSE$HTTP$ADMIN, password : Invalid password
Account : OSE$HTTP$ADMIN, password : INVALID
Account : OSM, password : OSM
Account : OSP22, password : OSP22
Account : OTA, password : OTA
Account : OUTLN, password : OUTLN
Account : OWA, password : OWA
Account : OWA_PUBLIC, password : OWA_PUBLIC
Account : OWF_MGR, password : OWF_MGR
Account : OWNER, password : OWNER
Account : OZF, password : OZF
Account : OZP, password : OZP
Account : OZS, password : OZS
Account : PA, password : PA
Account : PANAMA, password : PANAMA
Account : PATROL, password : PATROL
Account : PAUL, password : PAUL
Account : PERFSTAT, password : PERFSTAT
Account : PERSTAT, password : PERSTAT
Account : PJM, password : PJM
Account : PLANNING, password : PLANNING
Account : PLEX, password : PLEX
Account : PLSQL, password : SUPERSECRET

192.168.235.54 : Vulnerabilities

Account : PM, password : CHANGE_ON_INSTALL
Account : PM, password : UNKNOWN
Account : PM, password : PM
Account : PMI, password : PMI
Account : PN, password : PN
Account : PO, password : PO
Account : PO7, password : PO7
Account : PO8, password : PO8
Account : POA, password : POA
Account : POM, password : POM
Account : PORTAL_DEMO, password : PORTAL_DEMO
Account : PORTAL_SSO_PS, password : PORTAL_SSO_PS
Account : PORTAL30, password : PORTAL30
Account : PORTAL30, password : PORTAL31
Account : PORTAL30_ADMIN, password : PORTAL30_ADMIN
Account : PORTAL30_DEMO, password : PORTAL30_DEMO
Account : PORTAL30_PS, password : PORTAL30_PS
Account : PORTAL30_PUBLIC, password : PORTAL30_PUBLIC
Account : PORTAL30_SSO, password : PORTAL30_SSO
Account : PORTAL30_SSO_ADMIN, password : PORTAL30_SSO_ADMIN
Account : PORTAL30_SSO_PS, password : PORTAL30_SSO_PS
Account : PORTAL30_SSO_PUBLIC, password : PORTAL30_SSO_PUBLIC
Account : POS, password : POS
Account : POWERCARTUSER, password : POWERCARTUSER
Account : PRIMARY, password : PRIMARY
Account : PSA, password : PSA
Account : PSB, password : PSB
Account : PSP, password : PSP
Account : PUBSUB, password : PUBSUB
Account : PUBSUB1, password : PUBSUB1
Account : PV, password : PV
Account : QA, password : QA
Account : QDBA, password : QDBA
Account : QP, password : QP
Account : QS, password : CHANGE_ON_INSTALL
Account : QS, password : QS
Account : QS, password : UNKNOWN
Account : QS_ADM, password : CHANGE_ON_INSTALL
Account : QS_ADM, password : QS_ADM
Account : QS_ADM, password : UNKNOWN
Account : QS_CB, password : CHANGE_ON_INSTALL
Account : QS_CB, password : QS_CB
Account : QS_CB, password : UNKNOWN
Account : QS_CBADM, password : CHANGE_ON_INSTALL
Account : QS_CBADM, password : QS_CBADM
Account : QS_CBADM, password : UNKNOWN
Account : QS_CS, password : CHANGE_ON_INSTALL
Account : QS_CS, password : QS_CS
Account : QS_CS, password : UNKNOWN
Account : QS_ES, password : CHANGE_ON_INSTALL

192.168.235.54 : Vulnerabilities

Account : QS_ES, password : QS_ES
Account : QS_ES, password : UNKNOWN
Account : QS_OS, password : CHANGE_ON_INSTALL
Account : QS_OS, password : QS_OS
Account : QS_OS, password : UNKNOWN
Account : QS_WS, password : CHANGE_ON_INSTALL
Account : QS_WS, password : QS_WS
Account : QS_WS, password : UNKNOWN
Account : RE, password : RE
Account : REP_MANAGER, password : DEMO
Account : REP_OWNER, password : DEMO
Account : REP_OWNER, password : REP_OWNER
Account : REP_USER, password : DEMO
Account : REPADMIN, password : REPADMIN
Account : REPORTS_USER, password : OEM_TEMP
Account : REPORTS, password : REPORTS
Account : RG, password : RG
Account : RHX, password : RHX
Account : RLA, password : RLA
Account : RLM, password : RLM
Account : RMAIL, password : RMAIL
Account : RMAN, password : RMAN
Account : RRS, password : RRS
Account : SAMPLE, password : SAMPLE
Account : SAP, password : SAPR3
Account : SAP, password : 06071992
Account : SAPR3, password : SAP
Account : SCOTT, password : TIGER
Account : SCOTT, password : TIGGER
Account : SDOS_ICSAP, password : SDOS_ICSAP
Account : SECDEMO, password : SECDEMO
Account : SERVICECONSUMER1, password : SERVICECONSUMER1
Account : SH, password : CHANGE_ON_INSTALL
Account : SH, password : SH
Account : SH, password : UNKNOWN
Account : SITEMINDER, password : SITEMINDER
Account : SI_INFORMTN_SCHEMA, password : SI_INFORMTN_SCHEMA
Account : SLIDE, password : SLIDEPW
Account : SPIERSON, password : SPIERSON
Account : SSP, password : SSP
Account : STARTER, password : STARTER
Account : STRAT_USER, password : STRAT_PASSWD
Account : SWPRO, password : SWPRO
Account : SWUSER, password : SWUSER
Account : SYMPA, password : SYMPA
Account : SYS, password : CHANGE_ON_INSTALL
Account : SYS, password : D_SYSPW
Account : SYS, password : MANAGER
Account : SYS, password : ORACLE
Account : SYS, password : SYS

192.168.235.54 : Vulnerabilities

Account : SYS, password : SYSPASS
Account : SYS, password : MANAG3R
Account : SYS, password : ORACL3
Account : SYS, password : 0RACLE
Account : SYS, password : 0RACL3
Account : SYS, password : ORACLE8
Account : SYS, password : ORACLE9
Account : SYS, password : ORACLE8I
Account : SYS, password : ORACLE9I
Account : SYS, password : 0RACLE9I
Account : SYS, password : 0RACL39I
Account : SYSADM, password : SYSADM
Account : SYSADMIN, password : SYSADMIN
Account : SYSMAN, password : OEM_TEMP
Account : AMBU, password : hacschema
Account : QUEUE_USER, password : qmanager
Account : SYS, password : alLp0ver2
Account : SYSTEM, password : urA7mvP
Account : CHANGEMGR, password : datacontrol
Account : CCDEV, password : ccdev
Account : CCDBA, password : ccnulls
Account : CCDATA, password : ccdata
Account : CCFORMS, password : ccforms
Account : CCINTERFACE, password : ccinterface
Account : MCKHEO, password : mckheo
Account : CCREL, password : ccrel
Account : CCQUERY, password : ccquery
Account : CDXWEB, password : winplu5
Account : DRUG1, password : fdb3schema
Account : DRUG2, password : fdb3schema
Account : enc_ent, password : encent
Account : ENT, password : entpazz
Account : ENT_CONFIG, password : ent_configpazz
Account : ADF, password : adfpazz
Account : INF, password : infpazz
Account : INF_CONFIG, password : inf_configpazz
Account : SDM, password : sdmpazz
Account : STRMADM, password : pazzw0rd
Account : ENT_AUD, password : pazzw0rd
Account : ENT_ARCH, password : pazzw0rd
Account : POC_ARCH, password : pazzw0rd
Account : POC_AQ, password : qmanager
Account : INF_AQ, password : qmanager
Account : DATAMGR, password : datamgr
Account : CCUSER, password : bueno
Account : ALERTS, password : monitorhca
Account : HCALERTS, password : alertsuser
Account : AM, password : ampazz
Account : AM_AUD, password : pazzw0rd
Account : AUD, password : audpazz

192.168.235.54 : Vulnerabilities

Account : TMF, password : tmfpazz
Account : MN, password : mnpazz
Account : EH, password : ehpazz
Account : NG, password : ngpazz
Account : DM, password : dmpazz
Account : DMTOOL, password : dmtoolpazz
Account : STG_DMT, password : stg_dmtpazz
Account : WRL, password : wrlpazz
Account : NOTES, password : notespazz
Account : REPORTS, password : reportspazz
Account : ICONS, password : iconspazz
Account : BS, password : bspazz
Account : QZ, password : qzpazz
Account : RM, password : rmpazz
Account : RM_AUD, password : pazzw0rd
Account : COMMGR, password : commgrpazz
Account : OPSERVICE, password : opservicepazz
Account : SEC_CONFIG, password : sec_configpazz
Account : CTXSYS, password : ctxsyspazz
Account : OLOGY, password : ologypazz
Account : OLOGY_CONFIG, password : ology_configpazz
Account : DOC, password : docpazz
Account : DOC_CONFIG, password : doc_configpazz
Account : PORTAL, password : portal
Account : PORTAL_INSTALL, password : portal_install
Account : EBIDBADMIN, password : ebidbadmin
Account : DESIGN_OWNER, password : owb
Account : OWB_RUNTIME_REPOSITORY, password : owb
Account : RUNTIME_A_USER, password : owb

Suggestions:

Disable all the default accounts.

SMB NULL Session

Impact: Level 4 - Critical

CVE Reference: CVE-2002-1117

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 26920
Bugtraq ID: 494
CVE ID: 2002-1117

192.168.235.54 : Vulnerabilities

ISS X-Force ID: 10093
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Issue Description:

It is possible to log into the remote host using a SMB Null Session.

Suggestions:

Disable the use of SMB Null Sessions, should it not be a business requirement.

SMB Browse List Enumeration

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10397
Vendor URL: http://www.microsoft.com/

Issue Description:

An attacker will be able to obtain the remote browse list of the host. This can provide potential targets to an attacker.

Raw Scanner Output:

Plugin output :
Here is the browse list of the remote host :
CHE (os : 5.2)
CUSTER-40ECV65J (os : 5.2)
DUBCEK (os : 5.2)

Suggestions:

Netbios ports should never be accesible from the Internet and should be blocked on the firewall.

Comments:

192.168.235.54 : Vulnerabilities

Created On: 2009-12-22 10:42:27
Moderated to impact: medium
This issue was escalated due to the dangers associated with having SMB Browsing enabled across the Internet.

Business Document Files Available

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5560/TCP

Other References:

Nessus NASL ID : 11419

Issue Description:

Business document files was found on the website. These files may contain sensitive information that is not supposed to be available on the Internet. Please refer to 'details' for more information.

It is possible that of these Business document files contain sensitive information that is not suitable for public consumption. The files may have been accidently or purposefully published to the Internet.

Raw Scanner Output:

Plugin output :
The following office-related files are available on the remote server :
- Adobe Acrobat files (.pdf) :
/standaloneguide.pdf

Suggestions:

Verify that the information contained within the discovered Business document files do not contain information that should otherwise be restricted. Should files be found to contain information not suitable for public consumption it is recommended that these files be removed from anonymous viewing.

Business Document Files Available

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

192.168.235.54 : Vulnerabilities

Port/Protocol: 1158/TCP

Other References:

Nessus NASL ID : 11419

Issue Description:

Business document files was found on the website. These files may contain sensitive information that is not supposed to be available on the Internet. Please refer to 'details' for more information.

It is possible that of these Business document files contain sensitive information that is not suitable for public consumption. The files may have been accidently or purposefully published to the Internet.

Raw Scanner Output:

Plugin output :
The following office-related files are available on the remote server :
- Adobe Acrobat files (.pdf) :
/standaloneguide.pdf

Suggestions:

Verify that the information contained within the discovered Business document files do not contain information that should otherwise be restricted. Should files be found to contain information not suitable for public consumption it is recommended that these files be removed from anonymous viewing.

SMB Operating System Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10785

Issue Description:

It is possible to obtain information about the remote operating system.

Raw Scanner Output:

Plugin output :

192.168.235.54 : Vulnerabilities

The remote Operating System is : Windows Server 2003 3790 Service Pack 2
The remote native lan manager is : Windows Server 2003 5.2
The remote SMB Domain Name is : CUSTER-40ECV65J

Suggestions:

Informational plugin.

Unidentified Service

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 20034/TCP

Other References:

Nessus NASL ID : 11157

Issue Description:

An unknown service runs on this port as it was unable to fingerprint it. The service might have had its banner or response altered that the scan was unable to recognised the service.

However, services is sometimes opened by Trojan horses. Unless you know for sure what is behind it, you'd better check your system.

Raw Scanner Output:

Plugin output :
An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
NetBus 2.0 Pro
NetBus 2.0 Pro Hidden
NetRex
Whack Job
Netbus.444051
Unless you know for sure what is behind it, you'd better
check your system

Suggestions:

Determine the service that is running on this port and make sure the unknown service is required. Using an anti-virus scanner check that the service is not a Trojan. See details under the Control Panel for more information.

192.168.235.54 : Vulnerabilities

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 135/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Suggestions:

Informational plugin.

Oracle Database SID

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 22074

Issue Description:

The remote host is an Oracle Database server. Older versions of this server used to come bundled with the 'services' command. This command allows to list available SID on the database.

In addition this script tries to guest the SID name of the remote database by using default or common SID names.
An attacker may use these SIDs to get access to the remote database.

Raw Scanner Output:

192.168.235.54 : Vulnerabilities

Plugin output :
The following default sids have been found:
orcl
PLSExtProc

Suggestions:

Change the SID names from the default.

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1029/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Suggestions:

Informational plugin.

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

192.168.235.54 : Vulnerabilities

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Suggestions:

Informational plugin.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

Service detection

192.168.235.54 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1158/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1158/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :

192.168.235.54 : Vulnerabilities

The remote web server type is :
Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)

Suggestions:

Informational plugin.

Oracle TNSLNSR version query

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 10658
http://otn.oracle.com/deploy/security/pdf/listener_alert.pdf

Issue Description:

An Oracle tnslsnr service is listening on the remote port.

The remote host is running the Oracle tnslsnr service, a network interface to Oracle databases. This product allows a remote user to determine the presence and version number of a given Oracle installation.

Raw Scanner Output:

Plugin output :
A "version" request returns the following :
TNSLSNR for 32-bit Windows: Version 10.2.0.1.0 - Production
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
Oracle Bequeath NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
Windows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production,,

Suggestions:

Informational plugin.

OS Identification

192.168.235.54 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : Microsoft Windows Server 2003 Service Pack 2
Confidence Level : 99
Method : MSRPC
The remote host is running Microsoft Windows Server 2003 Service Pack 2

Suggestions:

Informational plugin.

NetBIOS Hostname Retrieval

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0621

Port/Protocol: 137/UDP

Other References:

Nessus NASL ID : 10150
CVE ID: 1999-0621
ISS X-Force ID: 8516
OVAL ID: 1024
Vendor URL: http://www.microsoft.com/

192.168.235.54 : Vulnerabilities

Issue Description:

The NetBIOS port is open (UDP:137). A remote attacker may use this to gain access to sensitive information such as computer name, workgroup/domain name, currently logged on user name, etc.

Raw Scanner Output:

Plugin output :
The following 4 NetBIOS names have been gathered :
CUSTER-40ECV65J = Computer name
WORKGROUP = Workgroup / Domain name
CUSTER-40ECV65J = File Server Service
WORKGROUP = Browser Service Elections
The remote host has the following MAC address on its adapter :
00:50:56:91:71:4a

Suggestions:

The NetBIOS port should only be open to internal networks. Block those ports from outside communication.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5560/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)

Suggestions:

Informational plugin.

192.168.235.54 : Vulnerabilities

SMB Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

Oracle Database Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 22073

Issue Description:

The remote host is running Oracle, a database server. It is possible to extract the version number of the remote installation by sending a 'VERSION' request to the remote TNS listener.

Raw Scanner Output:

Plugin output :

192.168.235.54 : Vulnerabilities

The remote Oracle TNS listener replies with the following version:
TNSLSNR for 32-bit Windows: Version 10.2.0.1.0 - Production
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
Oracle Bequeath NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
Windows NT Named Pipes NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production,,

Suggestions:

Informational plugin.

Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5580/TCP

Other References:

Nessus NASL ID : 11153

Issue Description:

This plugin attempts to identify the service running on the remote port.

Raw Scanner Output:

An Oracle Application Server is running on this port

Suggestions:

Informational plugin.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.54 : Vulnerabilities

Port/Protocol: 1158/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :
Date: Mon, 07 Dec 2009 19:46:33 GMT
Server: Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
Last-Modified: Tue, 30 Aug 2005 17:17:28 GMT
Accept-Ranges: bytes
Content-Length: 2919
Connection: Keep-Alive
Keep-Alive: timeout=15, max=100
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

192.168.235.54 : Vulnerabilities

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network
format)
The difference between the local and remote clocks is 303 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

192.168.235.54 : Vulnerabilities

A side effect of this feature is that the uptime of the remote host can be sometimes be computed.

Suggestions:

Informational plugin.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 3938/TCP

Other References:

Nessus NASL ID : 11032

192.168.235.54 : Vulnerabilities

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/e
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards

Suggestions:

It should be verified that no directories found, include sensitive information.

SMB Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 139/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

Virtual Directory Names Are Easily Guessable

192.168.235.54 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1158/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/dms0
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards

Suggestions:

It should be verified that no directories found, include sensitive information.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5560/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and

192.168.235.54 : Vulnerabilities

whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5520/TCP

Other References:

Nessus NASL ID : 11153

Issue Description:

This plugin attempts to identify the service running on the remote port.

Raw Scanner Output:

An Oracle Application Server is running on this port

Suggestions:

Informational plugin.

VMWare Host

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

192.168.235.54 : Vulnerabilities

Nessus NASL ID : 20094

Issue Description:

According to the MAC address of its network adapter, the remote host
is a VMWare virtual machine running.

Since it is physically accessible through the network, you should
ensure that its configuration matches the one of your corporate
security policy.

Suggestions:

Informational plugin.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

192.168.235.54 : Vulnerabilities

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.54 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.187.246
4.68.110.77
4.68.16.62
4.69.134.113
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.54

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 3938/TCP

Other References:

192.168.235.54 : Vulnerabilities

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 3938/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Headers :

192.168.235.54 : Vulnerabilities

Content-Type: text/html
charset=UTF-8
Transfer-Encoding: chunked
Connection: Keep-Alive
X-ORCL-EMSV: 10.1.0.4.1
X-ORCL-EMCT: 2009-12-07 14:46:36

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5560/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/dms0
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards

Suggestions:

It should be verified that no directories found, include sensitive information.

HyperText Transfer Protocol Information

192.168.235.54 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 5560/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :
Date: Mon, 07 Dec 2009 19:46:39 GMT
Server: Oracle Application Server Containers for J2EE 10g (9.0.4.1.0)
Last-Modified: Tue, 30 Aug 2005 17:17:28 GMT
Accept-Ranges: bytes
Content-Length: 2919
Connection: Keep-Alive
Keep-Alive: timeout=15, max=100
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

192.168.235.54 : Potential Vulnerabilities

Oracle Critical Patch Update - January 2009

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-2623, CVE-2008-3973, CVE-2008-3974, CVE-2008-3978, CVE-2008-3979, CVE-2008-3981, CVE-2008-3997, CVE-2008-3999, CVE-2008-4006, CVE-2008-4007, CVE-2008-4014, CVE-2008-4015, CVE-2008-4016, CVE-2008-4017, CVE-2008-5436, CVE-2008-5437, CVE-2008-5438, CVE-2008-5439, CVE-2008-5440, CVE-2008-5441, CVE-2008-5442, CVE-2008-5443, CVE-2008-5444, CVE-2008-5445, CVE-2008-5446, CVE-2008-5447, CVE-2008-5448, CVE-2008-5449, CVE-2008-5450, CVE-2008-5451, CVE-2008-5452, CVE-2008-5454, CVE-2008-5455, CVE-2008-5456, CVE-2008-5457, CVE-2008-5458, CVE-2008-5459, CVE-2008-5460, CVE-2008-5461, CVE-2008-5462, CVE-2008-5463

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95048
Bugtraq ID: 33177
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html

Issue Description:

Oracle Critical Patch Update (cpujan2009) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html

Malicious Software: NetBus Pro

Impact: Level 5 - Urgent

CVSS Score: 0

CVE Reference: CVE-1999-0660

192.168.235.54 : Potential Vulnerabilities

Port/Protocol: 20034/TCP

Other References:

Nessus NASL ID : 10152
CVE ID: 1999-0660
ISS X-Force ID: 1218, 1228, 2245, 2290, 3570, 3757, 5256, 8637
Snort Signature ID: 103, 107, 109, 110, 115, 117, 120, 121, 159, 195, 223, 224, 225, 226, 227, 229, 230, 231, 232, 233, 234, 235, 236, 237, 239, 240, 241, 320, 1843, 1853, 1854, 1855, 1856, 1980, 1981, 1982, 1983, 1984, 2100

Issue Description:

NetBus Pro is a remote administration tool that can be used for malicious purposes, such as sniffing what the user is typing, its passwords and so on.

An attacker may have installed it to control hosts on your network.

Suggestions:

This software should be removed immediately and is indicative of a possible compromise of the host. Best practice recommends that compromised hosts be rebuilt completely in case malware or rootkits have also been installed on the machine.

Oracle Critical Patch Update - April 2008

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-1811, CVE-2008-1812, CVE-2008-1813, CVE-2008-1814, CVE-2008-1815, CVE-2008-1816, CVE-2008-1817, CVE-2008-1818, CVE-2008-1819, CVE-2008-1820, CVE-2008-1821, CVE-2008-1822, CVE-2008-1823, CVE-2008-1824, CVE-2008-1825, CVE-2008-1826, CVE-2008-1827, CVE-2008-1828, CVE-2008-1829, CVE-2008-1830, CVE-2008-1831

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95045
Bugtraq ID: 28725
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

192.168.235.54 : Potential Vulnerabilities

Issue Description:

Oracle Critical Patch Update (cpuapr2008) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

Oracle Critical Patch Update - October 2008

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-2588, CVE-2008-2619, CVE-2008-2624, CVE-2008-2625, CVE-2008-3588, CVE-2008-3619, CVE-2008-3975, CVE-2008-3976, CVE-2008-3977, CVE-2008-3980, CVE-2008-3982, CVE-2008-3983, CVE-2008-3984, CVE-2008-3985, CVE-2008-3986, CVE-2008-3987, CVE-2008-3988, CVE-2008-3989, CVE-2008-3990, CVE-2008-3991, CVE-2008-3992, CVE-2008-3993, CVE-2008-3994, CVE-2008-3995, CVE-2008-3996, CVE-2008-3998, CVE-2008-4000, CVE-2008-4001, CVE-2008-4002, CVE-2008-4003, CVE-2008-4004, CVE-2008-4005, CVE-2008-4008, CVE-2008-4009, CVE-2008-4010, CVE-2008-4011, CVE-2008-4012, CVE-2008-4013

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95047
Bugtraq ID: 31683
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html

Issue Description:

Oracle Critical Patch Update (cpuoct2008) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-

192.168.235.54 : Potential Vulnerabilities

updates/cpuoct2008.html

Oracle Critical Patch Update - April 2007

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-2108, CVE-2007-2109, CVE-2007-2110, CVE-2007-2111, CVE-2007-2112, CVE-2007-2113, CVE-2007-2114, CVE-2007-2115, CVE-2007-2116, CVE-2007-2117, CVE-2007-2118, CVE-2007-2119, CVE-2007-2120, CVE-2007-2121, CVE-2007-2122, CVE-2007-2123, CVE-2007-2124, CVE-2007-2125, CVE-2007-2126, CVE-2007-2127, CVE-2007-2128, CVE-2007-2129, CVE-2007-2130, CVE-2007-2131, CVE-2007-2132, CVE-2007-2133, CVE-2007-2134

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95041
Bugtraq ID: 23532
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Issue Description:

Oracle Critical Patch Update (cpuapr2007) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Oracle Critical Patch Update - January 2008

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-0339

192.168.235.54 : Potential Vulnerabilities

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95044
Bugtraq ID: 27229
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

Issue Description:

Oracle Critical Patch Update (cpujan2008) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

Oracle Critical Patch Update - April 2006

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2006-0435, CVE-2006-1868, CVE-2006-1871, CVE-2006-1872, CVE-2006-1873, CVE-2006-1874, CVE-2006-3698, CVE-2006-3699, CVE-2006-3700, CVE-2006-3701, CVE-2006-3702, CVE-2006-3703, CVE-2006-3704, CVE-2006-3705, CVE-2006-3706, CVE-2006-3707, CVE-2006-3708, CVE-2006-3709, CVE-2006-3710, CVE-2006-3711, CVE-2006-3712, CVE-2006-3713, CVE-2006-3714, CVE-2006-3715, CVE-2006-3716, CVE-2006-3717, CVE-2006-3718, CVE-2006-3719, CVE-2006-3720, CVE-2006-3721, CVE-2006-3722, CVE-2006-3723, CVE-2006-3724

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95037
Bugtraq ID: 17590
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Issue Description:

Oracle Critical Patch Update (cpuapr2006) may be missing.

192.168.235.54 : Potential Vulnerabilities

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html

Oracle Critical Patch Update - October 2006

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2006-5332, CVE-2006-5333, CVE-2006-5334, CVE-2006-5335, CVE-2006-5336, CVE-2006-5337, CVE-2006-5338, CVE-2006-5339, CVE-2006-5340, CVE-2006-5341, CVE-2006-5342, CVE-2006-5343, CVE-2006-5344, CVE-2006-5345, CVE-2006-5346, CVE-2006-5347, CVE-2006-5348, CVE-2006-5349, CVE-2006-5350, CVE-2006-5351, CVE-2006-5352, CVE-2006-5353, CVE-2006-5354, CVE-2006-5355, CVE-2006-5356, CVE-2006-5357, CVE-2006-5358, CVE-2006-5359, CVE-2006-5360, CVE-2006-5361, CVE-2006-5362, CVE-2006-5363, CVE-2006-5364, CVE-2006-5365, CVE-2006-5366, CVE-2006-5367, CVE-2006-5368, CVE-2006-5369, CVE-2006-5370, CVE-2006-5371, CVE-2006-5372, CVE-2006-5373, CVE-2006-5374, CVE-2006-5375, CVE-2006-5376, CVE-2006-5377, CVE-2006-5378

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95039
Bugtraq ID: 20588
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Issue Description:

Oracle Critical Patch Update (cpuoct2006) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

192.168.235.54 : Potential Vulnerabilities

Oracle Critical Patch Update - January 2007

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2001-0729, CVE-2006-2940, CVE-2006-3738, CVE-2006-4339, CVE-2006-4343, CVE-2007-0222, CVE-2007-0268, CVE-2007-0269, CVE-2007-0270, CVE-2007-0271, CVE-2007-0272, CVE-2007-0273, CVE-2007-0274, CVE-2007-0275, CVE-2007-0276, CVE-2007-0277, CVE-2007-0278, CVE-2007-0279, CVE-2007-0280, CVE-2007-0281, CVE-2007-0282, CVE-2007-0283, CVE-2007-0284, CVE-2007-0285, CVE-2007-0286, CVE-2007-0287, CVE-2007-0288, CVE-2007-0289, CVE-2007-0290, CVE-2007-0291, CVE-2007-0292, CVE-2007-0293, CVE-2007-0294, CVE-2007-0295, CVE-2007-0296, CVE-2007-0297

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95040
Bugtraq ID: 22083
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

Issue Description:

Oracle Critical Patch Update (cpujan2007) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-4834, CVE-2008-4835, CVE-2008-4114

192.168.235.54 : Potential Vulnerabilities

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 35362
BID: 31179, 33121, 33122
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Issue Description:

It is possible to crash the remote host due to a flaw in SMB.

The remote host is vulnerable to memory corruption vulnerability in SMB which may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Suggestions:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008:
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Oracle Critical Patch Update - July 2006

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2006-3698, CVE-2006-3699, CVE-2006-3700, CVE-2006-3701, CVE-2006-3702, CVE-2006-3703, CVE-2006-3704, CVE-2006-3705, CVE-2006-3706, CVE-2006-3707, CVE-2006-3708, CVE-2006-3709, CVE-2006-3710, CVE-2006-3711, CVE-2006-3712, CVE-2006-3713, CVE-2006-3714, CVE-2006-3715, CVE-2006-3716, CVE-2006-3717, CVE-2006-3718, CVE-2006-3719, CVE-2006-3720, CVE-2006-3721, CVE-2006-3722, CVE-2006-3723, CVE-2006-3724

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95038
Bugtraq ID: 19054
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Issue Description:

Oracle Critical Patch Update (cpujul2006) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle

192.168.235.54 : Potential Vulnerabilities

Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html

Oracle Critical Patch Update - January 2006

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2005-0873, CVE-2005-2093, CVE-2005-2371, CVE-2005-2378, CVE-2006-0256, CVE-2006-0257, CVE-2006-0258, CVE-2006-0259, CVE-2006-0260, CVE-2006-0261, CVE-2006-0262, CVE-2006-0263, CVE-2006-0264, CVE-2006-0265, CVE-2006-0266, CVE-2006-0267, CVE-2006-0268, CVE-2006-0269, CVE-2006-0270, CVE-2006-0271, CVE-2006-0272, CVE-2006-0282, CVE-2006-0283, CVE-2006-0284, CVE-2006-0285, CVE-2006-0286, CVE-2006-0287, CVE-2006-0290, CVE-2006-0291, CVE-2006-0547, CVE-2006-0548, CVE-2006-0549, CVE-2006-0551, CVE-2006-0552, CVE-2006-0586

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95036
Bugtraq ID: 16287
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

Issue Description:

Oracle Critical Patch Update (cpujan2006) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644)

192.168.235.54 : Potential Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-4250

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 34477
BID: 31874

Issue Description:

The remote host is vulnerable to a buffer overrun in the 'Server' service.

This vulnerability may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Suggestions:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008:
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Oracle Critical Patch Update - July 2008

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2007-1359, CVE-2008-2576, CVE-2008-2577, CVE-2008-2578, CVE-2008-2579, CVE-2008-2580, CVE-2008-2581, CVE-2008-2582, CVE-2008-2583, CVE-2008-2586, CVE-2008-2587, CVE-2008-2589, CVE-2008-2590, CVE-2008-2591, CVE-2008-2592, CVE-2008-2593, CVE-2008-2594, CVE-2008-2595, CVE-2008-2596, CVE-2008-2597, CVE-2008-2598, CVE-2008-2599, CVE-2008-2600, CVE-2008-2601, CVE-2008-2602, CVE-2008-2603, CVE-2008-2604, CVE-2008-2605, CVE-2008-2606, CVE-2008-2607, CVE-2008-2608, CVE-2008-2609, CVE-2008-2610, CVE-2008-2611, CVE-2008-2612, CVE-2008-2613, CVE-2008-2614, CVE-2008-2615, CVE-2008-2616, CVE-2008-2617, CVE-2008-2618, CVE-2008-2620, CVE-2008-2621, CVE-2008-2622

Port/Protocol: 1521/TCP

Other References:

192.168.235.54 : Potential Vulnerabilities

Nessus NASL ID : 95046
Bugtraq ID: 30177
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

Issue Description:

Oracle Critical Patch Update (cpujul2008) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

Oracle Critical Patch Update - July 2007

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2007-3855, CVE-2007-3865, CVE-2007-3866, CVE-2007-3867

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95042
Bugtraq ID: 24887
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html

Issue Description:

Oracle Critical Patch Update (cpujul2007) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html

Oracle Critical Patch Update - October 2007

192.168.235.54 : Potential Vulnerabilities

Impact: Level 3 - High

CVSS Score: 7.8

CVE Reference: CVE-2007-5506

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95043
Bugtraq ID: 26103, 26101, 26108
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html

Issue Description:

Oracle Critical Patch Update (cpuoct2007) may be missing.

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html

Oracle Critical Patch Update - October 2005

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2005-0873

Port/Protocol: 1521/TCP

Other References:

Nessus NASL ID : 95035
Bugtraq ID: 15134
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Issue Description:

Oracle Critical Patch Update (cpuoct2008) may be missing.

192.168.235.54 : Potential Vulnerabilities

According to the version number of the Oracle listener program (tnslsnr) on the remote host, the Oracle Database may be missing a vendor supplied Critical Patch Update.

Suggestions:

Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

192.168.235.55 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
JAN
OS - OS Name
Windows 5.2
PORT - Port/Protocol/Service/Banner Information
445/tcp(cifs) none
PORT - Port/Protocol/Service/Banner Information
1025/tcp(dce-rpc) none
PORT - Port/Protocol/Service/Banner Information
23/tcp(telnet) none
PORT - Port/Protocol/Service/Banner Information
135/tcp(DCE) e1af82308-5d1f-11c2-22a4-08002b14a0fa none
PORT - Port/Protocol/Service/Banner Information
139/tcp(smb) none

Open Ports

Port	Protocol	Service	Comment
23	tcp	telnet	Service - Microsoft Windows XP telnetd
123	udp	ntp	Service - NTP
135	tcp	epmap	Service - Microsoft Windows RPC
137	udp	netbios-ns	Service - netbios-ns
138	udp	netbios-dgm	Service - netbios-dgm
139	tcp	netbios-ssn	Service - netbios-ssn
445	udp	microsoft-ds	Service - microsoft-ds
445	tcp	microsoft-ds	Service - Microsoft Windows 2003 microsoft-ds
500	udp	isakmp	Service - isakmp
1025	tcp	blackjack	Service - Microsoft Windows RPC

192.168.235.55 : Vulnerabilities

SMB Login

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0504, CVE-1999-0506, CVE-2000-0222, CVE-1999-0505, CVE-2002-1117, CVE-1999-0503, CVE-2005-3595

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10394
BID: 494, 990, 11199
Microsoft:
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP
CVE ID: 2002-1117
Generic Informational URL: http://www.sans.org/top20/oct02.php#W1
ISS X-Force ID: 10093, 17412
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0170.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0203.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0607.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0623.html
Mail List Post: http://archives.neohapsis.com/archives/vulndiscuss/2004-q3/0019.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00235.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00364.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Microsoft Knowledge Base Article: 143474
Microsoft Knowledge Base Article: 246261
Security Tracker: 1011344
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
Vendor URL: http://www.ibm.com/us/
Vendor URL: http://www.microsoft.com/

Issue Description:

This plugin attempts to log into the remote host using several username/password combinations. This however includes Null / Anonymous connections.

Raw Scanner Output:

Plugin output :
- NULL sessions are enabled on the remote host

192.168.235.55 : Vulnerabilities

Suggestions:

To fix this issue, edit the following key :
HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2.
Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.

SMB NULL Session

Impact: Level 4 - Critical

CVE Reference: CVE-2002-1117

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 26920
Bugtraq ID: 494
CVE ID: 2002-1117
ISS X-Force ID: 10093
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Issue Description:

It is possible to log into the remote host using a SMB Null Session.

Suggestions:

Disable the use of SMB Null Sessions, should it not be a business requirement.

Disabled SMB Signing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

192.168.235.55 : Vulnerabilities

Nessus NASL ID : 95184

Issue Description:

This host does not seem to be using SMB (Server Message Block) signing.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

Unauthorized users sniffing the network could catch many challege/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

Suggestions:

Workaround:
Please refer to Microsoft's article 887429 for information on enabling SMB signing.

Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95187

Issue Description:

The target Microsoft Windows Telnet server allows user credentials to be passed in clear text. By default, the service allows only integrated Windows NTLM authentication so that only authenticated Windows users/hosts from within the domain can login to the server.

With Telnet user credentials being passed in clear text, the target server becomes vulnerable to common attacks for password theft. This may occur through network sniffing or brute forcing user accounts on the server.

Suggestions:

Configure the service to accept NTLM authentication only for increased security during authentication. To learn how to configure Telnet NTLM Authentication, read Microsoft Knowledge Base article 201194.

Unencrypted Telnet Server

192.168.235.55 : Vulnerabilities

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 42263

Issue Description:

The remote Telnet server transmits traffic in cleartext.

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional data streams such as the X11 session.

Suggestions:

Disable this service and use SSH instead.

Comments:

Created On: 2009-12-22 10:44:29
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across the Internet.

SMB Browse List Enumeration

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10397
Vendor URL: http://www.microsoft.com/

Issue Description:

192.168.235.55 : Vulnerabilities

An attacker will be able to obtain the remote browse list of the host. This can provide potential targets to an attacker.

Raw Scanner Output:

Plugin output :
Here is the browse list of the remote host :
CHE (os : 5.2)
CUSTER-40ECV65J (os : 5.2)
DUBCEK (os : 5.2)
Other references : OSVDB:300

Suggestions:

Netbios ports should never be accesible from the Internet and should be blocked on the firewall.

Telnet Service and Version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 10281

Issue Description:

This detects the Telnet server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and types should be omitted where possible.

Raw Scanner Output:

Synopsis :
A Telnet server is listening on the remote port.
Description :
The remote host is running a Telnet server, a remote terminal server.
Solution :
Disable this service if you do not use it.
Risk factor :
None
Plugin output :

192.168.235.55 : Vulnerabilities

Here is the banner from the remote Telnet server :
---------- snip ----------
No more connections are allowed to telnet server. Please try again later.
---------- snip ----------

Suggestions:

Informational plugin.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

192.168.235.55 : Vulnerabilities

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Suggestions:

Informational plugin.

SMB Operating System Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10785

Issue Description:

It is possible to obtain information about the remote operating
system.

Raw Scanner Output:

Plugin output :
The remote Operating System is : Windows Server 2003 3790 Service Pack 1
The remote native lan manager is : Windows Server 2003 5.2
The remote SMB Domain Name is : CHE

192.168.235.55 : Vulnerabilities

Suggestions:

Informational plugin.

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 1025/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Suggestions:

Informational plugin.

DCE Services Identification

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 135/TCP

Other References:

Nessus NASL ID : 10736

Issue Description:

DCE services running on the remote can be enumerated by doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

192.168.235.55 : Vulnerabilities

Suggestions:

Informational plugin.

SMB Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 139/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet:
RST, FIN, ACK, FINIPSH.

192.168.235.55 : Vulnerabilities

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

NetBIOS Hostname Retrieval

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0621

Port/Protocol: 137/UDP

Other References:

Nessus NASL ID : 10150
CVE ID: 1999-0621

192.168.235.55 : Vulnerabilities

ISS X-Force ID: 8516
OVAL ID: 1024
Vendor URL: http://www.microsoft.com/

Issue Description:

The NetBIOS port is open (UDP:137). A remote attacker may use this to gain access to sensitive information such as computer name, workgroup/domain name, currently logged on user name, etc.

Raw Scanner Output:

Plugin output :
The following 6 NetBIOS names have been gathered :
CHE = Computer name
WORKGROUP = Workgroup / Domain name
CHE = File Server Service
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser
The remote host has the following MAC address on its adapter :
00:50:56:91:41:75

Suggestions:

The NetBIOS port should only be open to internal networks. Block those ports from outside communication.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

192.168.235.55 : Vulnerabilities

Remote operating system : Microsoft Windows Server 2003 Service Pack 1
Confidence Level : 99
Method : MSRPC
The remote host is running Microsoft Windows Server 2003 Service Pack 1

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.55 :
69.164.210.215
207.192.75.2
209.123.10.29
209.123.10.26
209.123.10.78
213.200.73.121
89.149.187.246
4.68.110.77
4.68.16.126
4.69.134.117
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157

192.168.235.55 : Vulnerabilities

64.230.137.250
192.168.235.55

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

SMB Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114

192.168.235.55 : Vulnerabilities

CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The ICMP timestamps seem to be in little endian format (not in network
format)
The difference between the local and remote clocks is 94 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

VMWare Host

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 20094

Issue Description:

According to the MAC address of its network adapter, the remote host
is a VMWare virtual machine running.

Since it is physically accessible through the network, you should
ensure that its configuration matches the one of your corporate
security policy.

Suggestions:

192.168.235.55 : Vulnerabilities

Informational plugin.

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

192.168.235.55 : Potential Vulnerabilities

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-4834, CVE-2008-4835, CVE-2008-4114

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 35362
BID: 31179, 33121, 33122
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Issue Description:

It is possible to crash the remote host due to a flaw in SMB.

The remote host is vulnerable to memory corruption vulnerability in SMB which may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Suggestions:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008:
http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644)

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-4250

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 34477
BID: 31874

192.168.235.55 : Potential Vulnerabilities

Issue Description:

The remote host is vulnerable to a buffer overrun in the 'Server' service.

This vulnerability may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Suggestions:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008:
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

192.168.235.56 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
bear
OS - OS Name
Ubuntu 6.06 Dapper Drake

Open Ports

Port	Protocol	Service	Comment
21	tcp	ftp	Banner - 220 ProFTPD 1.2.10 Server (Debian) [192.168.235.56]
22	tcp	ssh	Banner - SSH-1.99-OpenSSH_4.2
25	tcp	smtp	Banner - 421 4.3.2 Connection rate limit exceeded.
53	udp	domain	Service - ISC BIND 9.3.2
53	tcp	domain	Service - ISC BIND 9.3.2
137	udp	netbios-ns	Service - netbios-ns
138	udp	netbios-dgm	Service - netbios-dgm
139	tcp	netbios-ssn	Samba 3.X
445	tcp	microsoft-ds	Samba 3.X
587	tcp	submission	Sendmail 8.13.5.20060308/8.13.5/Debian-3ubuntu1

192.168.235.56 : Vulnerabilities

SMB Login

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0504, CVE-1999-0506, CVE-2000-0222, CVE-1999-0505, CVE-2002-1117, CVE-1999-0503, CVE-2005-3595

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10394
BID: 494, 990, 11199
Microsoft:
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP
CVE ID: 2002-1117
Generic Informational URL: http://www.sans.org/top20/oct02.php#W1
ISS X-Force ID: 10093, 17412
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0170.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0203.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0607.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2004-09/0623.html
Mail List Post: http://archives.neohapsis.com/archives/vulndiscuss/2004-q3/0019.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00235.html
Mail List Post: http://cert.uni-stuttgart.de/archive/bugtraq/2000/02/msg00364.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Microsoft Knowledge Base Article: 143474
Microsoft Knowledge Base Article: 246261
Security Tracker: 1011344
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
Vendor URL: http://www.ibm.com/us/
Vendor URL: http://www.microsoft.com/

Issue Description:

This plugin attempts to log into the remote host using several username/password combinations. This however includes Null / Anonymous connections.

Raw Scanner Output:

Plugin output :
- NULL sessions are enabled on the remote host

192.168.235.56 : Vulnerabilities

Suggestions:

To fix this issue, edit the following key :
HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2.
Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.

SMB Local User Enumeration

Impact: Level 5 - Urgent

CVSS Score: 7.5

CVE Reference: CVE-2000-1200, CVE-2002-1229

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10860
Bugtraq ID: 959, 5965
CERT VU: 482241
CVE ID: 2000-1200, 2002-1229
Generic Exploit URL: http://evgenii.rudnyi.ru/soft/sid/sid2user.cpp
Generic Exploit URL: http://mvb.saic.com/freeware/vmslt99b/nt/dom2sid.zip
Generic Informational URL:
http://www.cit.cornell.edu/computer/security/scanning/windows/nullsessions.html
Generic Informational URL: http://www.hsc.fr/ressources/articles/win_net_srv/ch04s06s10.html
Generic Informational URL: http://www.securityfocus.com/infocus/1352
ISS X-Force ID: 4015, 10374
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2000-01/0447.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2000-01/0462.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2002-10/0211.html
Mail List Post: http://archives.neohapsis.com/archives/ntbugtraq/1998/msg00162.html
Mail List Post: http://marc.theaimsgroup.com/?l=ntbugtraq&m=90222452931588&w=2
Microsoft Knowledge Base Article: q246261
Other Solution URL: http://www.ntbugtraq.com/default.aspx?pid=55&did=33
Packet Storm: http://packetstormsecurity.org/NT/hack/sid.zip
Related OSVDB ID: 714, 715
Vendor URL: http://www.microsoft.com/

Issue Description:

By using the host SID, it is possible to enumerates the local users on the remote Windows system. (we only enumerated users name whose ID is between 1000 and 2000 or whatever preferences you set).

Raw Scanner Output:

192.168.235.56 : Vulnerabilities

Plugin output :

- Administrator (id 500, Administrator account)
- nobody (id 501, Guest account)
- root (id 1000)
- root (id 1001)
- daemon (id 1002)
- daemon (id 1003)
- bin (id 1004)
- bin (id 1005)
- sys (id 1006)
- sys (id 1007)
- sync (id 1008)
- adm (id 1009)
- games (id 1010)
- tty (id 1011)
- man (id 1012)
- disk (id 1013)
- lp (id 1014)
- lp (id 1015)
- mail (id 1016)
- mail (id 1017)
- news (id 1018)
- news (id 1019)
- uucp (id 1020)
- uucp (id 1021)
- man (id 1025)
- proxy (id 1026)
- proxy (id 1027)
- kmem (id 1031)
- dialout (id 1041)
- fax (id 1043)
- voice (id 1045)
- cdrom (id 1049)
- floppy (id 1051)
- tape (id 1053)
- sudo (id 1055)
- audio (id 1059)
- dip (id 1061)
- www-data (id 1066)
- www-data (id 1067)
- backup (id 1068)
- backup (id 1069)
- operator (id 1075)
- list (id 1076)
- list (id 1077)
- irc (id 1078)
- irc (id 1079)
- src (id 1081)
- gnats (id 1082)
- gnats (id 1083)

192.168.235.56 : Vulnerabilities

- shadow (id 1085)
- utmp (id 1087)
- video (id 1089)
- sasl (id 1091)
- plugdev (id 1093)
- staff (id 1101)
- games (id 1121)
- cupsys (id 1200)

Suggestions:

Informational plugin.

SMB Host SID

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2000-1200, CVE-2002-1229

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10859
Bugtraq ID: 959, 5965
CERT VU: 482241
CVE ID: 2000-1200, 2002-1229
Generic Exploit URL: http://mvb.saic.com/freeware/vmslt99b/nt/dom2sid.zip
Generic Informational URL:
http://www.cit.cornell.edu/computer/security/scanning/windows/nullsessions.html
Generic Informational URL: http://www.hsc.fr/ressources/articles/win_net_srv/ch04s06s10.html
Generic Informational URL: http://www.securityfocus.com/infocus/1352
ISS X-Force ID: 4015, 10374
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2000-01/0447.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2000-01/0462.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2002-10/0211.html
Microsoft Knowledge Base Article: q246261
Other Solution URL: http://www.ntbugtraq.com/default.aspx?pid=55&did=33
Related OSVDB ID: 714
Vendor URL: http://www.microsoft.com/

Issue Description:

By emulating the call to LsaQueryInformationPolicy() it was
possible to obtain the host SID (Security Identifier).

192.168.235.56 : Vulnerabilities

The host SID can then be used to get the list of local users.

Raw Scanner Output:

Plugin output :
The remote host SID value is :
1-5-21-3874016443-2829349242-1787600336

Suggestions:

Informational plugin.

Microsoft Windows SMB Shares Unprivileged Access

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-1999-0519, CVE-1999-0520

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 42411
BID:8026
OSVDB:299

Issue Description:

It is possible to access a network share.

The remote has one or more Windows shares that can be accessed through the network with the given credentials.
Depending on the share rights, it may allow an attacker to read/write confidential data.

Suggestions:

To restrict access under Windows, open Explorer, do a right click on
each share, go to the 'sharing' tab, and click on 'permissions'.

SMB NULL Session

Impact: Level 4 - Critical

192.168.235.56 : Vulnerabilities

CVE Reference: CVE-2002-1117

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 26920
Bugtraq ID: 494
CVE ID: 2002-1117
ISS X-Force ID: 10093
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134395124579&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=103134930629683&w=2
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/238618.htm
Vendor Specific Advisory URL: http://seer.support.veritas.com/docs/239739.htm
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Issue Description:

It is possible to log into the remote host using a SMB Null Session.

Suggestions:

Disable the use of SMB Null Sessions, should it not be a business requirement.

Outdated SSH Protocol Versions Supported

Impact: Level 4 - Critical

CVE Reference: CVE-2001-0361, CVE-2001-1473 , CVE-2001-0572

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10882
Bugtraq ID: 2344
CERT VU: 61576, 997481, 888801, 161576
CIAC Advisory: I-047, m-017
CVE ID: 2001-0361, 2001-0572
Generic Informational URL: http://www.securityfocus.com/archive/1/161150
ISS X-Force ID: 6082
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2001-03/0225.html
Related OSVDB ID: 729
Snort Signature ID: 1324, 1325, 1326, 1327
Vendor Specific Advisory URL:

192.168.235.56 : Vulnerabilities

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_security_advisory09186a00800b168e.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
Vendor Specific Advisory URL: http://www.debian.org/security/2001/dsa-027

Issue Description:

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Suggestions:

If you use OpenSSH, set the option 'Protocol' to '2'.
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.

SSH Protocol Versions Supported.

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
- 1.33
- 1.5
- 1.99
- 2.0
SSHv1 host key fingerprint :
10:b9:b3:c0:80:96:a0:60:55:78:21:8d:26:82:eb:b3
SSHv2 host key fingerprint :
c2:95:e9:7e:01:02:6d:7f:f3:e8:b8:4b:8a:3b:79:40

Suggestions:

192.168.235.56 : Vulnerabilities

Informational plugin.

Usable Remote Name Server

Impact: Level 3 - High

CVSS Score: 5.8

CVE Reference: CVE-1999-0024

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 10539
Bugtraq ID: 136, 678
CERT: CA-1997-22
CVE ID: 1999-0024
ISS X-Force ID: 485

Issue Description:

The Name Server allows recursive queries to be performed. If this is your internal nameserver then forget this warning.

If this is a remote nameserver then it allows anyone to use it to resolve third parties names (such as www.nessus.org).This allows hackers to do cache poisoning attacks against this nameserver.

Suggestions:

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).
If you are using bind 8 you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf.
If you are using another name server consult its documentation.

DNS Amplification

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 53/UDP

192.168.235.56 : Vulnerabilities

Other References:

Nessus NASL ID : 35450
http://isc.sans.org/diary.html?storyid=5713

Issue Description:

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer which is bigger than the original request.

By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Suggestions:

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Disabled SMB Signing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 95184

Issue Description:

This host does not seem to be using SMB (Server Message Block) signing.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.

Unauthorized users sniffing the network could catch many challege/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

Suggestions:

Workaround:
Please refer to Microsoft's article 887429 for information on enabling SMB signing.

UDP Constant IP Identification Field Fingerprinting Vulnerability

192.168.235.56 : Vulnerabilities

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2002-0510

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 95152
Bugtraq ID: 4314

Issue Description:

The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.
Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported
that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

Suggestions:

We are not currently aware of any fixes for this issue.

FTP Supports Clear Text Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 34324

Issue Description:

The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

192.168.235.56 : Vulnerabilities

Suggestions:

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.

Comments:

Created On: 2009-12-22 12:44:39
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across open networks such as the Internet.

Enumerate Shares

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10395

Issue Description:

By connecting to the remote host using a null connection or guest access, an attacker will be able to enumerate all the shares on this host. Please refer to 'Details' for more information.

An attacker may be able to connect to some or all of the remote shares (if not properly protected) and access any information contained in those shares.
SMB shares should never be accesible from the Internet. If this host was scanned from the internal network, the impact is less and can be moderated accordingly.

Raw Scanner Output:

Plugin output :
Here are the SMB shares available on the remote host when logged as a NULL session:
- ADMIN$
- IPC$
- Shared
- print$

Suggestions:

Block the offending ports on the firewall if this host was scanned from the Internet.

192.168.235.56 : Vulnerabilities

SMB Browse List Enumeration

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10397
Vendor URL: http://www.microsoft.com/

Issue Description:

An attacker will be able to obtain the remote browse list of the host. This can provide potential targets to an attacker.

Raw Scanner Output:

Plugin output :
Here is the browse list of the remote host :
HIROHITO (os : 0.0)

Suggestions:

Netbios ports should never be accesible from the Internet and should be blocked on the firewall.

FTP Server type and version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 10092

Issue Description:

The login banner gives potential attackers additional information about the system they are attacking.

192.168.235.56 : Vulnerabilities

Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
The remote FTP banner is :
220 ProFTPD 1.2.10 Server (Debian) [192.168.235.56]

Suggestions:

Informational plugin.

SMB Operating System Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10785

Issue Description:

It is possible to obtain information about the remote operating
system.

Raw Scanner Output:

Plugin output :
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.22
The remote SMB Domain Name is : HIROHITO

Suggestions:

Informational plugin.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

192.168.235.56 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 587/TCP

Other References:

Nessus NASL ID : 14773

Issue Description:

This plugin attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...)

192.168.235.56 : Vulnerabilities

Raw Scanner Output:

Although this service answers with 3 digit ASCII codes
like FTP, SMTP or NNTP servers, Nessus was unable to identify it.
This is highly suspicious and might be a backdoor
 in this case,
your system is compromised and a cracker can control it remotely.
** If you know what it is, consider this message as a false alert
** and please report it to the Nessus team.
Solution : disinfect or reinstall your operating system
Risk factor : High

Suggestions:

None

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SMTP server is running on this port.

Suggestions:

Informational plugin.

SMB Detection

192.168.235.56 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 139/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

SAMBA Server Detection

192.168.235.56 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 25240
http://www.samba.org

Issue Description:

An SMB server is running on the remote host.

Suggestions:

Informational plugin.

NetBIOS Hostname Retrieval

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0621

Port/Protocol: 137/UDP

Other References:

Nessus NASL ID : 10150
CVE ID: 1999-0621
ISS X-Force ID: 8516
OVAL ID: 1024
Vendor URL: http://www.microsoft.com/

Issue Description:

The NetBIOS port is open (UDP:137). A remote attacker may use this to gain access to sensitive information such as computer name, workgroup/domain name, currently logged on user name, etc.

Raw Scanner Output:

Plugin output :
The following 7 NetBIOS names have been gathered :

192.168.235.56 : Vulnerabilities

HIROHITO = Computer name
HIROHITO = Messenger Service
HIROHITO = File Server Service
__MSBROWSE__ = Master Browser
MSHOME = Workgroup / Domain name
MSHOME = Master Browser
MSHOME = Browser Service Elections
This SMB server seems to be a SAMBA server (MAC address is NULL).

Suggestions:

The NetBIOS port should only be open to internal networks. Block those ports from outside communication.

DNS Server Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 11002

Issue Description:

A DNS server is running on this port. If you do not use it, disable it.

Suggestions:

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

192.168.235.56 : Vulnerabilities

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An FTP server is running on this port.

Suggestions:

Informational plugin.

SMB Password Policy Retrieval

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 17651

Issue Description:

It is possible to retrieve password policy using the supplied credentials

Using the supplied credentials it was possible to extract the password policy.

Raw Scanner Output:

Plugin output :
The following password policy is defined on the remote host:
Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800

192.168.235.56 : Vulnerabilities

Number of invalid logon before locked out (s): 0

Suggestions:

Ensure the password policy conforms to that of your businesses.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

192.168.235.56 : Vulnerabilities

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-1.99-OpenSSH_4.2
SSH supported authentication : publickey,password,keyboard-interactive

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.56 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.187.74

192.168.235.56 : Vulnerabilities

4.68.110.77
4.68.16.62
4.69.134.113
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
192.168.235.56

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

DNS Server Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 53/TCP

Other References:

Nessus NASL ID : 11002

Issue Description:

A DNS server is running on this port. If you do not use it, disable it.

Suggestions:

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.56 : Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

SMB share hosting office files

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 23974

Issue Description:

The remote share contains Office-related files

Raw Scanner Output:

Plugin output :
Here is a list of office files which have been found on the remote SMB
shares :
+ Shared :
- \Examples\oo-derivatives.doc
- \Examples\oo-about-ubuntu-ru.rtf
- \Examples\oo-trig.xls

192.168.235.56 : Vulnerabilities

Suggestions:

Ensure that any files containing confidential information have proper access controls set on them.

SMB Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 11011

Issue Description:

This script detects whether port 445 and 139 are open and if they are running SMB servers.

Port 445 is used for 'Netbios-less' communication between
two Windows 2000 hosts. An attacker may use it to obtain
and access shares, gain a list of usernames and so on...

Suggestions:

Informational plugin.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

192.168.235.56 : Vulnerabilities

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The difference between the local and remote clocks is -29 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

DNSSEC-aware Resolver

Impact: Level 1 - Low

CVE Reference: 0

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 35373

Issue Description:

The remote DNS resolver is DNSSEC-aware.

The remote DNS resolver accepts DNSSEC options. This means that it may verify the authenticity of DNSSEC protected zones if it is configured to trust their keys.

Suggestions:

This is an informational alert.

BIND version information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.56 : Vulnerabilities

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 10028
ISS X-ForceID: 197
Snort SignatureID: 257, 1616
Vendor URL: http://www.isc.org/

Issue Description:

It is possible to determine the version and type of a name daemon by querying a special "Question Name" on BIND based DNS servers.

Raw Scanner Output:

Plugin output :
The version of the remote DNS server is :
9.3.2

Suggestions:

Using the "version" directive in the "options" section will block the "version.bind" query, but it will not log such attempts.

SMTP Server type and version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 10263

Issue Description:

The SMTP Server's type and version can be detected by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

192.168.235.56 : Vulnerabilities

Plugin output :
Remote SMTP server banner :
220 localhost.localdomain ESMTP Sendmail 8.13.5.20060308/8.13.5/Debian-3ubuntu1
Mon, 7 Dec 2009 13:42:47 -0500
(No UCE/UBE) logging access from:
vps1.hackrack.co.za(OK)-vps1.hackrack.co.za [69.164.210.215]

Suggestions:

Informational plugin.

192.168.235.56 : Potential Vulnerabilities

Samba < 3.0.27 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4138, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2009-1888

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 28228
Bugtraq ID: 26455, 26454
CERT: TA07-352A
CVE ID: 2007-5398, 2007-4572
FrSIRT Advisory: ADV-2007-3869, ADV-2007-4238
ISS X-Force ID: 38502, 38501
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-11/0218.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-11/0219.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-11/0220.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-03/0152.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-06/0242.html
Other Advisory URL: http://lists.apple.com/archives/security-announce/2007/Dec/msg00002.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-November/000276.html
Other Advisory URL: http://secunia.com/secunia_research/2007-90/advisory/
Other Advisory URL: http://securityreason.com/securityalert/3372
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.447739
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-238251-1
Other Advisory URL: http://www.debian.org/security/2007/dsa-1409
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-29.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:224
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:224
Other Advisory URL: http://www.novell.com/linux/security/advisories/2007_65_samba.html
Other Advisory URL: http://www.ubuntu.com/usn/usn-544-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-544-2
Other Advisory URL: http://www.ubuntulinux.org/support/documentation/usn/usn-544-1
Other Advisory URL: https://lists.ubuntu.com/archives/ubuntu-security-announce/2008-June/000719.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00472.html
RedHat RHSA: RHSA-2007:1013, RHSA-2007:1016, RHSA-2007:1017
Related OSVDB ID: 39180, 1017399, 1016820, 39179
Secunia Advisory ID: 27450, 27691, 27682, 27679, 27720, 27701, 27731, 27787, 27742, 27927, 28136, 28368, 29341, 30484, 30835, 30736
Security Tracker: 1018953, 1018954
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307179

192.168.235.56 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307224
Vendor Specific Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-12/msg00003.html
Vendor Specific Advisory URL: http://lists.vmware.com/pipermail/security-announce/2008/000002.html
Vendor Specific Advisory URL: http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657
Vendor Specific News/Changelog Entry: http://docs.info.apple.com/article.html?artnum=307179
Vendor Specific News/Changelog Entry: http://us1.samba.org/samba/security/CVE-2007-4572.html
Vendor Specific News/Changelog Entry: http://us1.samba.org/samba/security/CVE-2007-5398.html
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1894
Vendor Specific Solution URL: http://www.apple.com/support/downloads/securityupdate20070091110411ppc.html
Vendor Specific Solution URL:
http://www.apple.com/support/downloads/securityupdate20070091110411universal.html
Vendor Specific Solution URL: http://www.apple.com/support/downloads/securityupdate2007009111051.html
Vendor Specific Solution URL: http://www.gentoo.org/security/en/glsa/glsa-200711-29.xml

Issue Description:

According to its banner, the version of the Samba server on the remote host contains a boundary error in the 'reply_netbios_packet()' function in 'nmbd/nmbd_packets.c' when sending NetBIOS replies.

Provided the server is configured to run as a WINS server, a remote attacker can exploit this issue by sending multiple specially-crafted WINS 'Name Registration' requests followed by a WINS 'Name Query' request, leading to a stack-based buffer overflow and allow for execution of arbitrary code. There is also a stack buffer overflow in nmbd's logon request processing code that can be triggered by means of specially-crafted GETDC mailslot requests when the affected server is configured as a Primary or Backup Domain Controller. Note that the Samba security team currently does not believe this particular can be exploited to execute arbitrary code remotely.

Suggestions:

Upgrade to Samba version 3.0.27 or later. Please see: http://www.samba.org

Samba < 3.0.25 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2009-1888

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 25217
Bugtraq ID: 23972, 23973, 23974, 24195, 24196, 24197, 24198
CERT VU: 268336, 773720

192.168.235.56 : Potential Vulnerabilities

CVE ID: 2007-2444, 2007-2446, 2007-2447
FrSIRT Advisory: ADV-2007-1805, ADV-2007-2210, ADV-2007-2281
Generic Exploit URL: http://www.metasploit.com
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0200.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0202.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0206.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0210.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0059.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0260.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-07/0070.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0246.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0247.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0248.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0249.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2007-05/0250.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2008-02/0119.html
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070502-01-P.asc
Other Advisory URL: http://docs.info.apple.com/article.html?artnum=306172
Other Advisory URL: http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
Other Advisory URL: http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00047.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00009.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-May/000187.html
Other Advisory URL: http://lists.suse.com/archive/suse-security-announce/2007-May/0006.html
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.475906
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102964-1
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200705-15.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-23.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:104
Other Advisory URL: http://www.trustix.org/errata/2007/0017/
Other Advisory URL: http://www.ubuntu.com/usn/usn-460-1
Other Advisory URL: http://www.zerodayinitiative.com/advisories/ZDI-07-029.html
Other Advisory URL: http://www.zerodayinitiative.com/advisories/ZDI-07-030.html
Other Advisory URL: http://www.zerodayinitiative.com/advisories/ZDI-07-031.html
Other Advisory URL: http://www.zerodayinitiative.com/advisories/ZDI-07-032.html
Other Advisory URL: http://www.zerodayinitiative.com/advisories/ZDI-07-033.html
RedHat RHSA: RHSA-2007:0354
Related OSVDB ID: 34699, 34700, 34698, 34731, 34732, 34733
Secunia Advisory ID: 25232, 25246, 25257, 25256, 25241, 25251, 25270, 25259, 25255, 25289, 25772, 25675, 25567, 25391, 26235, 26909, 27706, 28292, 26083
Snort Signature ID: 11442, 11443, 11444, 11445, 11446, 11447, 11448, 11449, 11450, 11451, 11452, 11453, 11454, 11455, 11456, 11457, 11458, 11459, 11460, 11461, 11462, 11463, 11464, 11465, 11466, 11467, 11468, 11469, 11470, 11471, 11472, 11473, 11474, 11475, 11476, 11477, 11478, 11479, 11480, 11481, 11482, 11483, 11484, 11485, 11486, 11487, 11488, 11489, 11490, 11491, 11492, 11493, 11494, 11495, 11496, 11497, 11498, 11499, 11500, 11501, 11502, 11503, 11504, 11505, 11506, 11507, 11508, 11509, 11510, 11511, 11512, 11513, 11514, 11515, 11516, 11517, 11518, 11519, 11520, 11521, 11522, 11523, 11524, 11525, 11526, 11527, 11528, 11529, 11530, 11531, 11532, 11533, 11534, 11535, 11536, 11537, 11538, 11539, 11540, 11541, 11542, 11543, 11544, 11545, 11546, 11547, 11548, 11549, 11550, 11551, 11552, 11553, 11554, 11555, 11556, 11557, 11558, 11559, 11560, 11561, 11562, 11563, 11564, 11565, 11566, 11567, 11568, 11569, 11570, 11571, 11572, 11573,

192.168.235.56 : Potential Vulnerabilities

11574, 11575, 11576, 11577, 11578, 11579, 11580, 11581, 11582, 11583, 11584, 11585, 11586, 11587, 11588, 11589, 11590, 11591, 11592, 11593, 11594, 11595, 11596, 11597, 11598, 11599, 11600, 11601, 11602, 11603, 11604, 11605, 11606, 11607, 11608, 11609, 11610, 11611, 11612, 11613, 11614, 11615, 12984, 12985, 12986, 12987, 12988, 12989, 12990, 12991, 12992, 12993, 12994, 12995, 12996, 12997, 12998, 12999, 13000, 13001, 13002, 13003, 13004, 13005, 13006, 13007, 13008, 13009, 13010, 13011, 13012, 13013, 13014, 13015, 13016, 13017, 13018, 13019, 13020, 13021, 13022, 13023, 13024, 13025, 13026, 13027, 13028, 13029, 13030, 13031, 13032, 13033, 13034, 13035, 13036, 13037, 13038, 13039, 13040, 13041, 13042, 13043, 13044, 13045, 13046, 13047, 13048, 13049, 13050, 13051, 13052, 13053, 13054, 13055, 13056, 13057, 13058, 13059, 13060, 13061, 13062, 13063, 13064, 13065, 13066, 13067, 13068, 13069, 13070, 13071, 13072, 13073, 13074, 13075, 13076, 13077, 13078, 13079, 13080, 13081, 13082, 13083, 13084, 13085, 13086, 13087, 13088, 13089, 13090, 13091, 13092, 13093, 13094, 13095, 13096, 13097, 13098, 13099, 13100, 13101, 13102, 13103, 13104, 13105, 13106, 13107, 13108, 13109, 13110, 13111, 13112, 13113, 13114, 13115, 13116, 13117, 13118, 13119, 13120, 13121, 13122, 13123, 13124, 13125, 13126, 13127, 13128, 13129, 13130, 13131, 13132, 13133, 13134, 13135, 13136, 13137, 13138, 13139, 13140, 13141, 13142, 13143, 13144, 13145, 13146, 13147, 13148, 13149, 13150, 13151, 13152, 13153, 13154, 13155, 13156, 13157, 13367, 13368, 13369, 13370, 13371, 13372, 13373, 13374, 13375, 13376, 13377, 13378, 13379, 13380, 13381, 13382, 13383, 13384, 13385, 13386, 13387, 13388, 13389, 13390, 13391, 13392, 13393, 13394, 13395, 13396, 13397, 13398, 13399, 13400, 13401, 13402, 13403, 13404, 13405, 13406, 13407, 13408, 13409, 13410, 13411, 13412, 13413, 13414, 14900, 14988
Vendor Specific Advisory URL: http://www8.itrc.hp.com/service/cki/docDisplay.do?docId=c01067768
Vendor Specific News/Changelog Entry: http://www.samba.org/samba/security/CVE-2007-2446.html
Vendor Specific News/Changelog Entry: http://www.samba.org/samba/security/CVE-2007-2447.html
Vendor Specific News/Changelog Entry: http://www.xerox.com/downloads/usa/en/c/cert_XRX08_001.pdf
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1366
Vendor URL: http://www.samba.org

Issue Description:

According to its banner, the version of the Samba server installed on the remote host is affected by multiple buffer overflow and remote command injection vulnerabilities.

The vulnerabilities can be exploited remotely, as well as allow local privilege escalation.

Suggestions:

Upgrade to Samba version 3.0.25 or later. Please see: http://www.samba.org

Samba < 3.0.24 Multiple Flaws

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2004-0082, CVE-2004-0186, CVE-2004-0600, CVE-2004-0686, CVE-2004-0807, CVE-2004-0808, CVE-2004-0815, CVE-2004-0882, CVE-2004-0930, CVE-2004-1154, CVE-2004-2546, CVE-2006-1059, CVE-2006-3403, CVE-2007-0452, CVE-2007-0453, CVE-2007-0454, CVE-2007-2444, CVE-2007-2446, CVE-2007-2447, CVE-2007-4572, CVE-2007-5398, CVE-2007-6015, CVE-2009-1888

192.168.235.56 : Potential Vulnerabilities

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 24685
Bugtraq ID: 22395, 22403, 22410, 18927
CVE ID: 2007-0453, 2007-0452, 2007-0454
FrSIRT Advisory: ADV-2007-0483
ISS X-Force ID: 32231
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-02/0038.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-02/0039.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-02/0045.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-04/0113.html
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070201-01-P.asc
Other Advisory URL: http://fedoranews.org/cms/node/2579
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-February/000142.html
Other Advisory URL: http://lists.suse.com/archive/suse-security-announce/2007-Feb/0002.html
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.476916
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200702-01.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:034
Other Advisory URL: http://www.trustix.org/errata/2007/0007/
Other Advisory URL: http://www.ubuntu.com/usn/usn-419-1
Other Advisory URL: http://www.us.debian.org/security/2007/dsa-1257
RedHat RHSA: RHSA-2007:0060
Related OSVDB ID: 33101, 33100
Secunia Advisory ID: 24043, 24151, 24101, 24046, 24060, 24021, 24030, 24067, 24076, 24145, 24140, 24188, 24284, 24792
Security Tracker: 1017589
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.476916
Vendor Specific Advisory URL: http://www.trustix.org/errata/2007/0007
Vendor Specific News/Changelog Entry: http://us1.samba.org/samba/security/CVE-2007-0453.html
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1005
Vendor Specific Solution URL: http://itrc.hp.com/service/cki/docDisplay.do?docId=c00943462

Issue Description:

According to its version number, the remote Samba server is affected by several flaws.

The following flaws are reported:
- A denial of service issue occurring if an authenticated attacker sends a large number of CIFS session requests which will cause an infinite loop to occur in the smbd daemon, thus utilizing CPU resources and denying access to legitimate users ;
- A remote format string vulnerability which may be exploited by an attacker with write access to a remote share by sending a malformed request to the remote service (this issue only affects installations sharing an AFS file system when the afsacl.so VFS module is loaded) - A remote buffer overflow vulnerability affecting the NSS lookup capability of the remote winbindd daemon

192.168.235.56 : Potential Vulnerabilities

Suggestions:

Upgrade to Samba 3.0.24 or newer. Please see: http://www.samba.org

OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2006-5051, CVE-2006-5052 , CVE-2008-4109, CVE-2006-4924

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22466
Bugtraq ID: 20241, 20245
CVE ID: 2006-5051, 2008-4109, 2006-5052
ISS X-Force ID: 29254, 45202
Mail List Post: http://lists.debian.org/debian-security-announce/2008/msg00227.html
Other Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-527.htm
Other Advisory URL: http://www-unix.globus.org/mail_archive/security-announce/2007/04/msg00000.html
Other Advisory URL: http://www.debian.org/security/2008/dsa-1638
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1189
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1212
RedHat RHSA: RHSA-2006:0697-9, RHSA-2006:0698, RHSA-2006:0697
Secunia Advisory ID: 22173, 22196, 22183, 22236, 22158, 22208, 22245, 22270, 22362, 22352, 22487, 22495, 22823, 22926, 23680, 24805, 24799, 31885, 32080, 32181, 28320
Security Tracker: 1020891
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20061001-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=305214
Vendor Specific Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00004.html
Vendor Specific Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Oct/0005.html
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-216.htm
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200611-06.xml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:179
Vendor Specific Advisory URL: http://www.openbsd.org/errata.html#ssh
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-355-1
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-649-1
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=498678
Vendor Specific News/Changelog Entry: http://marc.theaimsgroup.com/?l=openbsd-cvs&m=115589252024127&w=2
Vendor Specific News/Changelog Entry: http://openssh.org/txt/release-4.4

192.168.235.56 : Potential Vulnerabilities

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host contains a race condition that may allow an unauthenticated remote attacker to crash the service or, on portable OpenSSH, possibly execute code on the affected host.

In addition, another flaw exists that may allow an attacker to determine the validity of usernames on some platforms. Note that successful exploitation of these issues requires that GSSAPI authentication be enabled.

Suggestions:

Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org

[DSA1222] DSA-1222-2 proftpd

Impact: Level 5 - Urgent

CVSS Score: 7.5

CVE Reference: CVE-2006-5815, CVE-2006-6170, CVE-2006-6171

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 23757
http://www.debian.org/security/2006/dsa-1222
BID:0
DSA:1222

Issue Description:

The remote host is missing the DSA-1222 security update

Suggestions:

No suggestion at this time

ProFTP Buffer Overflow Vulnerability

Impact: Level 5 - Urgent

CVE Reference: CVE-2006-5815

192.168.235.56 : Potential Vulnerabilities

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 27055
Bugtraq ID: 20992
CVE ID: 2006-5815
FrSIRT Advisory: ADV-2006-4451
ISS X-Force ID: 30147
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0442.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0455.html
Mail List Post: http://attrition.org/pipermail/vim/2006-November/001150.html
Mail List Post: http://whitestar.linuxbox.org/pipermail/exploits/2006-November/000059.html
Other Advisory URL: http://gleg.net/vulndisco_meta.shtml
Other Advisory URL: http://www.gleg.net/proftpd.txt
Other Advisory URL: http://www.trustix.org/errata/2006/0070/
Secunia Advisory ID: 22803, 23184, 23179, 23174, 23207, 23329
Security Tracker: 1017167
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.502491
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200611-26.xml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:217-1
Vendor Specific Advisory URL: http://www.us.debian.org/security/2006/dsa-1222
Vendor Specific News/Changelog Entry: http://bugs.proftpd.org/show_bug.cgi?id=2858
Vendor URL: http://www.proftpd.org/

Issue Description:

The remote ProFTPD server is prone to a buffer overflow attack.

According to its banner, the version of ProFTPD installed on the remote host contains an off-by-one string manipulation flaw in its "sreplace" function. An attacker may be able to leverage this issue to crash the affected service or execute arbitrary code remotely, subject to the privileges under which the application operates.

Suggestions:

Upgrade to ProFTPD version 1.3.0a or later. Please see: http://www.proftpd.org

Samba < 3.0.35 / 3.2.13 / 3.3.6 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2009-1886, CVE-2009-1888

192.168.235.56 : Potential Vulnerabilities

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 39502

Issue Description:

The remote Samba server may be affected by a security bypass vulnerability.

According to its version number, the version of Samba running on the remote host has a security bypass vulnerability. Access restrictions can be bypassed due to a read of uninitialized data in smbd. This could allow a user to modify an access control list (ACL), even when they should be denied permission. Note the 'dos filemode' parameter must be set to 'yes' in smb.conf in order for an attack to be successful (the default setting is 'no').
Also note versions 3.2.0 - 3.2.12 of smbclient are affected by a format string vulnerability, though Nessus has not checked for this.

Suggestions:

Upgrade to Samba version 3.3.6 / 3.2.13 / 3.0.35 or later, or apply the appropriate patch referenced in the vendor's advisory.

SAMBA 3.0 < 3.0.35

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2004-2546, CVE-2006-3403, CVE-2007-0453, CVE-2007-0454, CVE-2007-6015, CVE-2008-1105, CVE-2004-0082, CVE-2004-0808, CVE-2007-2446, CVE-2004-0686, CVE-2004-0807, CVE-2004-1154, CVE-2006-1059, CVE-2007-5398, CVE-2007-2447, CVE-2007-2444, CVE-2004-0930, CVE-2004-0186, CVE-2004-0600, CVE-2007-0452, CVE-2008-4314, CVE-2004-0815, CVE-2004-0882, CVE-2007-4138, CVE-2007-4572

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95131

Issue Description:

SAMBA 3.0 version is older than 3.0.35.

192.168.235.56 : Potential Vulnerabilities

According to the version number of the SAMBA banner on the remote host, the SAMBA 3.0 version may be vulnerable to a number of flaws, some of which allow code execution.
These include the following:
CVE-2004-2546
CVE-2006-3403
CVE-2007-0453
CVE-2007-0454
CVE-2007-6015
CVE-2008-1105
CVE-2004-0082
CVE-2004-0808
CVE-2007-2446
CVE-2004-0686
CVE-2004-0807
CVE-2004-1154
CVE-2006-1059
CVE-2007-5398
CVE-2007-2447
CVE-2007-2444
CVE-2004-0930
CVE-2004-0186
CVE-2004-0600
CVE-2007-0452
CVE-2008-4314
CVE-2004-0815
CVE-2004-0882
CVE-2007-4138
CVE-2007-4572

Suggestions:

Upgrade to the latest version of Samba 3.0. Please see: http://www.samba.org

Samba < 3.0.28 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2007-6015, CVE-2009-1888

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 29253

192.168.235.56 : Potential Vulnerabilities

Bugtraq ID: 26791
CVE ID: 2007-6015
FrSIRT Advisory: ADV-2007-4153
ISS X-Force ID: 38965
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-12/0118.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-12/0125.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-12/0193.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-03/0152.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-06/0242.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-12/msg00006.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-December/000287.html
Other Advisory URL: http://lists.vmware.com/pipermail/security-announce/2008/000005.html
Other Advisory URL: http://secunia.com/secunia_research/2007-99/advisory/
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.451554
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-238251-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-520.htm
Other Advisory URL: http://www.debian.org/security/2007/dsa-1427
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200712-10.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:244
Other Advisory URL: http://www.novell.com/linux/security/advisories/2007_68_samba.html
Other Advisory URL: http://www.ubuntu.com/usn/usn-556-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-December/msg00308.html
RedHat RHSA: RHSA-2007:1114, RHSA-2007:1117
Secunia Advisory ID: 27760, 27993, 28029, 28003, 28067, 27977, 28028, 28037, 27894, 27999, 28089, 28891, 29032, 29341, 30484, 30835
Security Tracker: 1019065
Snort Signature ID: 13291
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307430
Vendor Specific Advisory URL: http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657
Vendor Specific News/Changelog Entry: http://bugs.gentoo.org/show_bug.cgi?id=200773
Vendor Specific News/Changelog Entry: http://support.avaya.com/elmodocs2/security/ASA-2007-520.htm
Vendor Specific News/Changelog Entry: http://www.samba.org/samba/security/CVE-2007-6015.html
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1976

Issue Description:

According to its banner, the version of the Samba server on the remote host is reportedly affected by a boundary error in 'nmbd' within the 'send_mailslot' function.

Provided the 'domain logons' option is enabled in 'smb.conf', an attacker can leverage this issue to produce a stack-based buffer overflow using a 'SAMLOGON' domain logon packet in which the username string is placed at an odd offset and is followed by a long 'GETDC' string. Note that Nessus has not actually tried to exploit this issue nor verify whether the 'domain logons' option has been enabled on the remote host.

Suggestions:

Upgrade to Samba version 3.0.28 or later. Please see: http://www.samba.org

192.168.235.56 : Potential Vulnerabilities

WINS Domain Controller Spoofing Vulnerability

Impact: Level 4 - Critical

CVSS Score: 7.6

CVE Reference: CVE-1999-1593

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 95165
Bugtraq ID: 2221

Issue Description:

Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server and is also supported by Samba server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network.
Unfortunately, WINS does not properly verify the registration of Domain Controllers (DCs).
It's possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.

By exploting this vulnerability, an unauthorized user can cause the WINS service to redirect requests for a domain controller to a different system, which could lead to a loss of network functionality. The user may also be able to retrieve username and password hashes.

Suggestions:

The following workaround was provided by David Byrne :
The best workaround I could think of is to use static entries for records that are sensitive (there are probably more besides 1Ch). Domain Controllers shouldn't be changed very often, so the management work would be minimal.
The following workaround was provided by Paul L Schmehl :
MS's response was that because WINS uses NetBIOS, which has no security capabilities, there was no way to prevent that sort of hijacking. Their answer is Active Directory, Kerberos and DNS.

BIND 9 Denial of Service Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

192.168.235.56 : Potential Vulnerabilities

CVE Reference: CVE-2006-4095, CVE-2006-4096, CVE-2006-2073, CVE-2007-0494, CVE-2006-2937, CVE-2006-2940

Port/Protocol: 53/TCP

Other References:

Nessus NASL ID : 22311
Bugtraq ID: 19859, 17692, 22231, 20248, 20247
CERT VU: 915404, 697164
CVE ID: 2006-4095, 2006-4096
FrSIRT Advisory: ADV-2006-3473
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.481241
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200609-11.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:163
Other Advisory URL: http://www.openbsd.org/errata.html
Other Advisory URL: http://www.ubuntu.com/usn/usn-343-1
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1172
Other Advisory URL: https://issues.rpath.com/browse/RPL-626
Related OSVDB ID: 28558, 28557
Secunia Advisory ID: 21752, 21790, 21786, 21816, 21835, 21818, 21828, 21838, 21926, 21912, 21954, 22298, 25402
Security Tracker: 1016794
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=305530
Vendor Specific Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Oct/0001.html
Vendor Specific Advisory URL: http://security.freebsd.org/advisories/FreeBSD-SA-06:20.bind.asc
Vendor Specific Advisory URL: http://www.isc.org/sw/bind/bind-security.php
Vendor Specific Advisory URL: http://www.trustix.org/errata/2006/0051/

Issue Description:

The version of BIND installed on the remote host suggests that it suffers from multiple denial of service vulnerabilities, which may be triggered by either by sending a large volume of recursive queries or queries for SIG records where there are multiple SIG(covered) RRsets.

Note that the scanner obtained the version by sending a special DNS request for the text 'version.bind' in the domain 'chaos', the value of which can be and sometimes is tweaked by DNS administrators.

Suggestions:

Upgrade to BIND 9.4.0b2 / 9.3.3rc2 / 9.3.2-P1 / 9.2.7rc2 / 9.2.6-P1 or later. Please see: http://www.isc.org

Sendmail < 8.13.2 Mail X-Header Handling Remote Overflow

Impact: Level 4 - Critical

192.168.235.56 : Potential Vulnerabilities

CVSS Score: 5

CVE Reference: CVE-2009-1490

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 38877
http://www.nmrc.org/~thegnome/blog/apr09/
http://www.sendmail.org/releases/8.13.2
BID:34944
OSVDB:54669

Issue Description:

The remote mail server is affected by a buffer overflow
vulnerability.

Suggestions:

No suggestion at this time

Samba < 3.0.30 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 8.5

CVE Reference: CVE-2008-1105, CVE-2008-4314, CVE-2009-1888, CVE-2008-4189

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 32476
Bugtraq ID: 29404, 31255
CVE ID: 2008-1105, 2008-4189
FrSIRT Advisory: ADV-2008-1681
ISS X-Force ID: 45251
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0354.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-06/0242.html
Mail List Post: http://attrition.org/pipermail/vim/2008-October/002082.html
Other Advisory URL: http://lists.debian.org/debian-security-announce/2008/msg00168.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-06/msg00000.html
Other Advisory URL: http://lists.vmware.com/pipermail/security-announce/2008/000023.html

192.168.235.56 : Potential Vulnerabilities

Other Advisory URL: http://secunia.com/secunia_research/2008-20/
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.473951
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0180
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200805-23.xml
Other Advisory URL: https://lists.ubuntu.com/archives/ubuntu-security-announce/2008-June/000719.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-May/msg01082.html
Secunia Advisory ID: 30228, 30385, 30442, 30396, 30449, 30478, 30489, 30543, 30736, 30835, 30802, 31246, 31911, 33696
Security Tracker: 1020123
Snort Signature ID: 13901
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-249086-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT2163
Vendor Specific Advisory URL: http://www.xerox.com/downloads/usa/en/c/cert_XRX08_009.pdf
Vendor Specific Advisory URL: http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01475657
Vendor Specific News/Changelog Entry: http://www.samba.org/samba/security/CVE-2008-1105.html

Issue Description:

According to its banner, the version of the Samba server on the remote host is reportedly affected by a boundary error in 'nmbd' within the 'receive_smb_raw' function in 'lib/util_sock.c' when parsing SMB packets received in a client context.

By sending specially-crafted packets to an 'nmbd' server configured as a local or domain master browser, an attacker can leverage this issue to produce a heap-based buffer overflow and execute arbitrary code with system privileges. Note that Nessus has not actually tried to exploit this issue, verify the remote 'nmbd' server's configuration, or determine if the fix has been applied.

Suggestions:

Upgrade to Samba version 3.0.30. Please see: http://www.samba.org

MS00-047: NetBIOS Name Server Protocol Spoofing patch (269239)

Impact: Level 4 - Critical

CVSS Score: 5

CVE Reference: CVE-2000-0673

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 10482
http://support.microsoft.com/support/kb/articles/q299/4/44.asp
http://www.microsoft.com/technet/security/bulletin/ms00-047.mspx

192.168.235.56 : Potential Vulnerabilities

BID:1514
OSVDB:381

Issue Description:

It is possible to spoof the netbios name.

Suggestions:

No suggestion at this time

ProFTPD Command Truncation Cross-Site Request Forgery

Impact: Level 4 - Critical

CVSS Score: 6.8

CVE Reference: CVE-2008-4242

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 34265
http://archives.neohapsis.com/archives/fulldisclosure/2008-09/0524.html
http://bugs.proftpd.org/show_bug.cgi?id=3115
BID:31289
OSVDB:48411

Issue Description:

The remote FTP server is prone to a cross-site request forgery attack.

Suggestions:

No suggestion at this time

[DSA1218] DSA-1218-1 proftpd

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2006-6563, CVE-2006-6171

192.168.235.56 : Potential Vulnerabilities

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 23704
http://www.debian.org/security/2006/dsa-1218
BID:0
DSA:1218

Issue Description:

The remote host is missing the DSA-1218 security update

Suggestions:

No suggestion at this time

Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities

Impact: Level 3 - High

CVSS Score: 6

CVE Reference: CVE-2009-2813, CVE-2009-2906, CVE-2009-2948

Port/Protocol: 445/TCP

Other References:

Nessus NASL ID : 41970
http://www.samba.org/samba/security/CVE-2009-2906.html
http://www.samba.org/samba/security/CVE-2009-2948.html
http://www.samba.org/samba/security/CVE-2009-2813.html
BID:36572, 36573
OSVDB:57955, OSVDB:58519, OSVDB:58520

Issue Description:

The remote Samba server may be affected by multiple vulnerabilities.

According to its banner, the version of Samba server on the remote
host is earlier than 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2. Such versions are potentially affected by multiple
issues :
- If a user in '/etc/passwd' is misconfigured to have an empty home directory, then connecting to the
home share of this user will use the root of the file system as the home directory. (CVE-2009-2813)
- Specially crafted SMB requests on authenticated SMB connections can send smbd into a 100% loop, causing
a denial of service. (CVE-2009-2906)

192.168.235.56 : Potential Vulnerabilities

- When 'mount.cifs' is installed as a setuid program, a user can pass it a credential or password path to which he or she does not have access and then use the '--verbose' option to view the first line of that file. (CVE-2009-2948)

Suggestions:

Upgrade to Samba 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 or later.

ISC BIND 9 EVP_VerifyFinal() / DSA_do_verify() SSL/TLS Signature Validation Weakness

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2009-0025

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 38735
https://www.isc.org/node/389

Issue Description:

The remote name server is affected by a signature validation weakness.

According to its version number, the remote installation of BIND does not properly check the return value from the OpenSSL library functions 'EVP_VerifyFinal()' and 'DSA_do_verify()'. A remote attacker may be able to exploit this weakness to spoof answers returned from zones for signature checks on DSA and ECDSA keys used with SSL / TLS.

Suggestions:

Upgrade to BIND 9.3.6-P1 / 9.4.3-P1 / 9.5.1-P1 / 9.6.0-P1 or later.

OpenSSH X11 Session Hijacking Vulnerability

Impact: Level 3 - High

CVE Reference: CVE-2008-1483

192.168.235.56 : Potential Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 31737
Bugtraq ID: 28444
Secunia Advisory ID 229522, 29537, 29554, 29626, 29627, 29676, 29683, 29686, 29721, 29735, 29873, 29939, 30086, 30230, 30249, 30347, 30361, 31531, 31882
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01462841
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3137
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
Vendor Specific News/Changelog Entry: http://sourceforge.net/project/shownotes.php?release_id=590180

Issue Description:

According to its banner, the version of SSH installed on the remote host is older than 5.0.

Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

Suggestions:

Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org

ISC BIND 9 DNSSEC Cache Poisoning

Impact: Level 3 - High

CVSS Score: 4

CVE Reference: CVE-2009-4022

Port/Protocol: 53/TCP

Other References:

Nessus NASL ID : 42983

Suggestions:

No suggestion at this time

ISC BIND Dynamic Update Message Handling Remote DoS

192.168.235.56 : Potential Vulnerabilities

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2009-0696

Port/Protocol: 53/TCP

Other References:

Nessus NASL ID : 40422

Suggestions:

No suggestion at this time

TCP Sequence Number Approximation

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-0230

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 12213
Bugtraq ID: 10183
CERT VU: 415294
CERT: CA-2001-09, TA04-111A
CVE ID: 2004-0230
FrSIRT Advisory: ADV-2006-3983
Generic Exploit URL: http://www.osvdb.org/ref/04/04030-exploit.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/disconn.py
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/Kreset.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp_rfc31337-compliant.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/tcp_reset.c
Generic Exploit URL: http://www.packetstormsecurity.org/0405-exploits/autoRST.c
Generic Exploit URL: http://www.packetstormsecurity.org/cisco/ttt-1.3r.tar.gz
Generic Informational URL: http://nytimes.com/aponline/technology/AP-Internet -Threat.html
Generic Informational URL:

192.168.235.56 : Potential Vulnerabilities

http://slashdot.org/articles/04/04/20/1738217.shtml?tid=126&tid=128&tid=172&tid=95
Generic Informational URL: http://www.cnn.com/2004/TECH/internet/04/20/internet.threat/index.html
Generic Informational URL: http://www.eweek.com/article2/0,1759,1571185,00.asp
Generic Informational URL: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
Generic Informational URL: http://www.ietf.org/rfc/rfc0793.txt
Generic Informational URL: http://www.msnbc.msn.com/id/4788445/
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.ppt
ISS X-Force ID: 15886
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0028.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0029.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108302060014745&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108506952116653&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
Microsoft Knowledge Base Article: 922819
Microsoft Security Bulletin: MS05-019
Microsoft Security Bulletin: MS06-064
Other Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3/SCOSA-2005.3.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9/SCOSA-2005.9.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Other Advisory URL: http://www.jpcert.or.jp/at/2004/at040003.txt
Other Advisory URL: http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx
Other Advisory URL: http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
Other Advisory URL: http://www.seil.jp/en/ann/announce_en_20040421_01.txt
Other Advisory URL: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Other Advisory URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/170
Other Solution URL: http://isc.sans.org/diary.php?date=2004-04-20
OVAL ID: 4791, 2689, 3508, 270
Related OSVDB ID: 6094, 29429, 4030
Secunia Advisory ID: 11448, 11447, 11443, 11444, 11445, 11462, 11458, 11682, 11679, 12682, 14946, 22341, 14170, 11440
Snort Signature ID: 2523
US-CERT Cyber Security Alert: TA04-111A
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2005.05.02.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
Vendor Specific Advisory URL: http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
Vendor Specific Advisory URL: http://www.juniper.net/support/alert.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/niscc-236929.txt
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1535

192.168.235.56 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
Vendor Specific News/Changelog Entry: http://www.juniper.net/support/alert.html
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc

Issue Description:

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc.).

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks.

Suggestions:

Please see http://www.securityfocus.com/bid/10183/solution, for the right solution for your infrastructure.

[DSA1164] DSA-1164-1 sendmail

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2006-4434

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 22706
http://www.debian.org/security/2006/dsa-1164
BID:19714
DSA:1164

Issue Description:

The remote host is missing the DSA-1164 security update

Suggestions:

No suggestion at this time

192.168.235.56 : Potential Vulnerabilities

ProFTPd User Enumeration

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-1602

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 15484
Bugtraq ID: 11430
CVE ID: 2004-1602
ISS X-Force ID: 17724
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-10/0145.html
Other Advisory URL: http://security.lss.hr/index.php?page=details&ID=LSS-2004-10-02
Secunia Advisory ID: 12836
Security Tracker: 1011687
Vendor URL: http://www.proftpd.org/

Issue Description:

The remote ProFTPd server is as old or older than 1.2.10 It is possible to determine which user names are valid on the remote host based on timing analysis attack of the login procedure. An attacker may use this flaw to set up a list of valid usernames for a more efficient brute-force attack against the remote host.

A timing attack is described in ProFTPD that could assist a remote user in enumerating usernames. A remote attacker may exploit this vulnerability to determine what usernames are valid, privileged, or do not exist on the remote system.

Raw Scanner Output:

Synopsis :
The remote FTP server may disclose the list of valid usernames.
Description :
The remote ProFTPd server is as old or older than 1.2.10
It is possible to determine which user names are valid on the remote host
based on timing analysis attack of the login procedure.
An attacker may use this flaw to set up a list of valid usernames for a
more efficient brute-force attack against the remote host.
Solution :
Upgrade to a newer version.
Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

192.168.235.56 : Potential Vulnerabilities

CVE : CVE-2004-1602
BID : 11430
Other references : OSVDB:10758

Suggestions:

Update software to newest version. Please see: http://www.proftpd.org

DNS Server Allows Remote Clients to Snoop the DNS Cache

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 95228

Issue Description:

The DNS server was found to allow DNS cache snooping. This means, any attacker could remotely check if a given domain name is cached on the DNS server.
This issue occurs when a target DNS server allows an untrusted client to make non-recursive DNS queries for domains that the target DNS server is not authoritative on. If the target DNS server consults its cache and replies with a valid answer (the IP address or "does not exist" NXDOMAIN reply), it is vulnerable to this attack. This tells the attacker that someone from the target network recently resolved that particular domain name.

DNS caches are short lived and are generated by a recent DNS name-resolution event. By repeatedly monitoring DNS cache entries over a period of time, an attacker could gain a variety of information about the target network. For example, one could analyze Web-browsing habits of the users of a network. By querying for DNS MX record caches, one could check for email communication between two companies. Information gathered from the DNS cache could lead to a variety of consequences ranging from an invasion of privacy to corporate espionage. The above mentioned paper presents a couple of attack scenarios where this vulnerability can be used.

Suggestions:

Here is a suggested solution for the Microsoft Windows DNS server. One rigorous solution involves what is known popularly as a "split DNS" configuration.
The idea is to have two separate DNS servers, one for the DMZ/perimeter of the network that faces the public Internet, while the other is internal and not publically accessible.
The external one has zone information about only the hosts in the DMZ region which need to be accessed from the Internet. It has no information about the internal hosts with non-routable addresses.
The internal one has all the authoritative information about the internal hosts, and also static entries

192.168.235.56 : Potential Vulnerabilities

for the services in the DMZ region (so internal users can access those if required).
Typically, the internal DNS server will be Active Directory integrated, with (secure) dynamic updates enabled.
The external DNS server will typically be a standalone (not integrated with the Active Directory) server without any dynamic DNS updates enabled.
To prevent the unrelated DNS cache-poisoning vulnerability, also configure the registry as explained in the QID 15037 on both the DNS servers.
Both the DNS servers can be named with identical domain names, such as example.com without any conflicts.
The external DNS server should be set as a "forwarder" in the DNS settings of the internal DNS server.
This means, for any DNS query (A/PTR) that the internal DNS server receives, that it is not able to resolve, it forwards it to the external DNS server for resolution.
Through the "DNS" MMC snap-in, Recursion should be enabled on the external DNS server, and disabled in the internal one. This prevents the internal DNS server from attempting to resolve DNS queries if the external one fails to do so.
To reinforce the last configuration, the internal DNS server should be set as a "slave" DNS server through the "HKEY_LOCAL_MACHINESYSTEM CurrentControlSetServicesDNSParameters" key's "IsSlave" value set to 1.
Finally, to prevent cache snooping on the external DNS server, create a "MaxCacheTtl" DWORD entry with value set to 1 under the "HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesDNSParameters" key of the external DNS server. This makes the TTL of any cached DNS entry on the external DNS server equal to 1 second, effectively disabling caching on it. Since for any query originating from the internal network, both the DNS servers cache the responses, performance is not affected at all even by disabling the external cache - repeated future DNS queries will be picked up by the internal DNS server and replied to from its cache.
This separates the external DNS proxy from the internal DNS cache, and prevents any DNS cache snooping from the public Internet.
For BIND and the understanding of the issue this URL will be helpful.
http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

OpenSSH < 5.2/5.2p1

Impact: Level 2 - Medium

CVSS Score: 1.2

CVE Reference: CVE-2008-3259

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95122
Bugtraq ID: 30339
CVE ID: 2008-3259
FrSIRT Advisory: ADV-2008-2148
ISS X-Force ID: 43940
Secunia Advisory ID: 31179

192.168.235.56 : Potential Vulnerabilities

Security Tracker: 1020537
Vendor Specific News/Changelog Entry: http://openssh.com/security.html
Vendor Specific News/Changelog Entry: http://www.openssh.com/txt/release-5.1

Issue Description:

OpenSSH version is older than 5.2/5.2p1.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.2, is below:
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

ISC BIND 9 hostname.bind Map Disclosure

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 53/UDP

Other References:

Nessus NASL ID : 35371

Issue Description:

It is possible to learn the remote host name by querying the remote BIND 9.x server for 'hostname.bind'
in the CHAOS domain.

Raw Scanner Output:

Synopsis :
The DNS server discloses the remote host name.
Description :
It is possible to learn the remote host name by querying the remote
DNS server for 'hostname.bind' in the CHAOS domain.
Solution :
It may be possible to disable this feature. Consult the vendor's
documentation for more information.
Risk factor :
None
Plugin output :

192.168.235.56 : Potential Vulnerabilities

The remote host name is :
hirohito

Suggestions:

Specify 'hostname none;' in the remote server's 'named.conf' to disable this feature.

192.168.235.57 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
Fedora Core 5
PORT - Port/Protocol/Service/Banner Information
22/tcp(ssh) SSH-2.0-OpenSSH_4.3
PORT - Port/Protocol/Service/Banner Information
57161/tcp(rpc-status) none
PORT - Port/Protocol/Service/Banner Information
111/tcp(rpc-portmapper) none

Open Ports

Port	Protocol	Service	Comment
22	tcp	ssh	Banner - SSH-2.0-OpenSSH_4.3
111	udp	sunrpc	Service - RPC Portmapper
111	tcp	sunrpc	Service - RPC Portmapper
57161	tcp	unknown	Unknown

192.168.235.57 : Vulnerabilities

UDP packets with source port of 53 bypass firewall rules

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-1473

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 11580
Bugtraq ID: 11237
CERT VU: 329230
CVE ID: 2004-1473
ISS X-Force ID: 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 12635
Security Tracker: 1011388, 1011389
Vendor Specific Advisory URL:
http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor URL: http://www.symantec.com/

Issue Description:

It is possible to by-pass the rules of the remote firewall by sending UDP packets with a source port equal to 53.

An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall.

Suggestions:

Review your firewall rules policy and ensure that your firewall is stateful (tracks the state of allowed connections).

TCP Sequence Number Approximation

Impact: Level 3 - High

CVSS Score: 5

192.168.235.57 : Vulnerabilities

CVE Reference: CVE-2004-0230

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 12213
Bugtraq ID: 10183
CERT VU: 415294
CERT: CA-2001-09, TA04-111A
CVE ID: 2004-0230
FrSIRT Advisory: ADV-2006-3983
Generic Exploit URL: http://www.osvdb.org/ref/04/04030-exploit.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/disconn.py
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/Kreset.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp_rfc31337-compliant.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/tcp_reset.c
Generic Exploit URL: http://www.packetstormsecurity.org/0405-exploits/autoRST.c
Generic Exploit URL: http://www.packetstormsecurity.org/cisco/ttt-1.3r.tar.gz
Generic Informational URL: http://nytimes.com/aponline/technology/AP-Internet -Threat.html
Generic Informational URL:
http://slashdot.org/articles/04/04/20/1738217.shtml?tid=126&tid=128&tid=172&tid=95
Generic Informational URL: http://www.cnn.com/2004/TECH/internet/04/20/internet.threat/index.html
Generic Informational URL: http://www.eweek.com/article2/0,1759,1571185,00.asp
Generic Informational URL: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
Generic Informational URL: http://www.ietf.org/rfc/rfc0793.txt
Generic Informational URL: http://www.msnbc.msn.com/id/4788445/
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.ppt
ISS X-Force ID: 15886
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0028.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0029.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108302060014745&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108506952116653&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
Microsoft Knowledge Base Article: 922819
Microsoft Security Bulletin: MS05-019
Microsoft Security Bulletin: MS06-064
Other Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3/SCOSA-2005.3.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9/SCOSA-2005.9.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Other Advisory URL: http://www.jpcert.or.jp/at/2004/at040003.txt
Other Advisory URL: http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx

192.168.235.57 : Vulnerabilities

Other Advisory URL: http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
Other Advisory URL: http://www.seil.jp/en/ann/announce_en_20040421_01.txt
Other Advisory URL: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Other Advisory URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/170
Other Solution URL: http://isc.sans.org/diary.php?date=2004-04-20
OVAL ID: 4791, 2689, 3508, 270
Related OSVDB ID: 6094, 29429, 4030
Secunia Advisory ID: 11448, 11447, 11443, 11444, 11445, 11462, 11458, 11682, 11679, 12682, 14946, 22341, 14170, 11440
Snort Signature ID: 2523
US-CERT Cyber Security Alert: TA04-111A
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2005.05.02.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
Vendor Specific Advisory URL: http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
Vendor Specific Advisory URL: http://www.juniper.net/support/alert.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/niscc-236929.txt
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1535
Vendor Specific Advisory URL: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
Vendor Specific News/Changelog Entry: http://www.juniper.net/support/alert.html
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc

Issue Description:

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc.).

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks.

Suggestions:

Please see http://www.securityfocus.com/bid/10183/solution, for the right solution for your infrastructure.

SSH Protocol Versions Supported.

192.168.235.57 : Vulnerabilities

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
 - 1.99
 - 2.0
SSHv2 host key fingerprint :
11:5e:2a:8a:09:44:6d:9b:d3:47:da:c4:69:09:d5:ab

Suggestions:

Informational plugin.

Hidden RPC Services

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 95171

Issue Description:

The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.
When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the

192.168.235.57 : Vulnerabilities

portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

Raw Scanner Output:

Name: portmap/rpcbind
Program: 100000
Version: 2
Protocol: tcp
Port: 111

Suggestions:

Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.

192.168.235.57 : Vulnerabilities

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.57 : Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-2.0-OpenSSH_4.3
SSH supported authentication : publickey,gssapi-with-mic,password

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 111 :
 - program: 100000 (portmapper), version: 2

Suggestions:

192.168.235.57 : Vulnerabilities

Informational plugin.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP
The remote host is running Linux Kernel 2.6

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 57161/TCP

Other References:

Nessus NASL ID : 11111

192.168.235.57 : Vulnerabilities

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 57161 :
- program: 100024 (status), version: 1

Suggestions:

Informational plugin.

RPC portmapper

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0632

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 10223

Issue Description:

Determines whether the remote RPC portmapper is installed or not. If it is installed then its presence will be noted as a knowledge base item and will be used by the other scripts.

Suggestions:

Informational plugin.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

192.168.235.57 : Vulnerabilities

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The difference between the local and remote clocks is -12511 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

192.168.235.57 : Vulnerabilities

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.57 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.187.74
4.68.110.77
4.68.16.126
4.69.134.117
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.57

Suggestions:

192.168.235.57 : Vulnerabilities

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 111 :

192.168.235.57 : Vulnerabilities

- program: 100000 (portmapper), version: 2

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32768/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32768 :
- program: 100024 (status), version: 1

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

192.168.235.57 : Vulnerabilities

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

192.168.235.57 : Potential Vulnerabilities

OpenSSH < 5.0

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2000-0999, CVE-2001-0572, CVE-2001-1029, CVE-2005-2797, CVE-2005-2798, CVE-2006-0225, CVE-2006-4924, CVE-2006-4925, CVE-2006-5051, CVE-2006-5052, CVE-2006-5229, CVE-2006-5794, CVE-2007-2243, CVE-2007-3102, CVE-2007-4752, CVE-2008-1483, CVE-2008-1657, CVE-2008-3234, CVE-2008-3259, CVE-2008-4109, CVE-2008-5161

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95134

Issue Description:

OpenSSH version is older than 5.0.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.0, is below:
CVE-2000-0999 - OpenBSD ssh Format String Privilege Escalation
CVE-2001-0572 - Cisco Devices SSH Password Length Disclosure, SSH Traffic Analysis Connection Attributes Disclosure
CVE-2001-1029 - OpenSSH on FreeBSD libutil Arbitrary File Read
CVE-2005-2797 - OpenSSH Multiple X11 Channel Forwarding Leaks
CVE-2005-2798 - OpenSSH GSSAPIAuthentication Credential Escalation
CVE-2006-0225 - OpenSSH scp Command Line Filename Processing Command Injection
CVE-2006-4924 - OpenSSH Identical Block Packet DoS
CVE-2006-4925 - OpenSSH packet.c Invalid Protocol Sequence Remote DoS
CVE-2006-5051 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2006-5052 - OpenSSH GSSAPI Authentication Abort Username Enumeration
CVE-2006-5229 - OpenSSH Username Password Complexity Account Enumeration
CVE-2006-5794 - OpenSSH Privilege Separation Monitor Weakness
CVE-2007-2243 - OpenSSH S/KEY Authentication Account Enumeration
CVE-2007-3102 - OpenSSH linux_audit_record_event Crafted Username Audit Log Injection
CVE-2007-4752 - OpenSSH Trusted X11 Cookie Connection Policy Bypass
CVE-2008-1483 - OpenSSH X11 Forwarding Local Session Hijacking
CVE-2008-1657 - OpenSSH ~/.ssh/rc ForceCommand Bypass Arbitrary Command Execution
CVE-2008-3234 - OpenSSH on Debian sshd Crafted Username Arbitrary Remote SELinux Role Access
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
CVE-2008-4109 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution

192.168.235.57 : Potential Vulnerabilities

CVE-2008-5161 - OpenSSH CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure, SSH Tectia Multiple Products CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: www.openssh.org

Multiple Linux Vendor rpc.statd Remote Format String Vulnerability

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2000-0666

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 10544
mmoReferences
http://online.securityfocus.com/bid/1480

Issue Description:

mmoVulnDescV
The rpc.statd program is part of the nfs-utils packages, distributed with a number of popular Linux distributions. The rpc.statd server is an RPC server that implements the Network Status and Monitor RPC protocol. It's a component of the Network File System (NFS) architecture. A format string vulnerability in some implementations of this service allow for a remote root shell compromise.

mmoSecConcerns
The logging code in rpc.statd uses the syslog() function passing it as the format string user supplied data. A malicious user can construct a format string that injects executable code into the process address space and overwrites a function's return address, thus forcing the program to execute the code. rpc.statd requires root privileges for opening its network socket, but fails to drop these privileges later on. Thus code executed by the malicious user will execute with root privileges.

Suggestions:

mmoSuggestion
Upgrade to the latest version of rpc.statd (see references)

OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities

192.168.235.57 : Potential Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2006-5051, CVE-2006-5052 , CVE-2008-4109, CVE-2006-4924

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22466
Bugtraq ID: 20241, 20245
CVE ID: 2006-5051, 2008-4109, 2006-5052
ISS X-Force ID: 29254, 45202
Mail List Post: http://lists.debian.org/debian-security-announce/2008/msg00227.html
Other Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-527.htm
Other Advisory URL: http://www-unix.globus.org/mail_archive/security-announce/2007/04/msg00000.html
Other Advisory URL: http://www.debian.org/security/2008/dsa-1638
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1189
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1212
RedHat RHSA: RHSA-2006:0697-9, RHSA-2006:0698, RHSA-2006:0697
Secunia Advisory ID: 22173, 22196, 22183, 22236, 22158, 22208, 22245, 22270, 22362, 22352, 22487, 22495, 22823, 22926, 23680, 24805, 24799, 31885, 32080, 32181, 28320
Security Tracker: 1020891
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20061001-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=305214
Vendor Specific Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00004.html
Vendor Specific Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Oct/0005.html
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-216.htm
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200611-06.xml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:179
Vendor Specific Advisory URL: http://www.openbsd.org/errata.html#ssh
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-355-1
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-649-1
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=498678
Vendor Specific News/Changelog Entry: http://marc.theaimsgroup.com/?l=openbsd-cvs&m=115589252024127&w=2
Vendor Specific News/Changelog Entry: http://openssh.org/txt/release-4.4

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host contains a race condition that may allow an unauthenticated remote attacker to crash the service or, on portable OpenSSH, possibly execute code on the affected host.

In addition, another flaw exists that may allow an attacker to determine the validity of usernames on

192.168.235.57 : Potential Vulnerabilities

some platforms. Note that successful exploitation of these issues requires that GSSAPI authentication be enabled.

Suggestions:

Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org

OpenSSH X11 Session Hijacking Vulnerability

Impact: Level 3 - High

CVE Reference: CVE-2008-1483

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 31737
Bugtraq ID: 28444
Secunia Advisory ID 229522, 29537, 29554, 29626, 29627, 29676, 29683, 29686, 29721, 29735, 29873, 29939, 30086, 30230, 30249, 30347, 30361, 31531, 31882
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01462841
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3137
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
Vendor Specific News/Changelog Entry: http://sourceforge.net/project/shownotes.php?release_id=590180

Issue Description:

According to its banner, the version of SSH installed on the remote host is older than 5.0.

Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

Suggestions:

Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org

OpenSSH < 5.2/5.2p1

Impact: Level 2 - Medium

CVSS Score: 1.2

192.168.235.57 : Potential Vulnerabilities

CVE Reference: CVE-2008-3259

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95122
Bugtraq ID: 30339
CVE ID: 2008-3259
FrSIRT Advisory: ADV-2008-2148
ISS X-Force ID: 43940
Secunia Advisory ID: 31179
Security Tracker: 1020537
Vendor Specific News/Changelog Entry: http://openssh.com/security.html
Vendor Specific News/Changelog Entry: http://www.openssh.com/txt/release-5.1

Issue Description:

OpenSSH version is older than 5.2/5.2p1.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.2, is below:
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

192.168.235.58 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
mx1
OS - OS Name
Windows 5.2
PORT - Port/Protocol/Service/Banner Information
443/tcp(www) Microsoft-IIS 6.0
PORT - Port/Protocol/Service/Banner Information
21/tcp(ftp) 220 Microsoft FTP Service
PORT - Port/Protocol/Service/Banner Information
25/tcp(smtp) 220 mail.pcidemo Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Mon, 7 Dec 2009 15:13:42 -0500
PORT - Port/Protocol/Service/Banner Information
80/tcp(www) Microsoft-IIS 6.0

Open Ports

Port	Protocol	Service	Comment
21	tcp	ftp	Banner - 220 Microsoft FTP Service
25	tcp	smtp	Banner - 220 cook.asvtestbed.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Mon, 7 Dec 2009 09:26:12 -0500
80	tcp	http	Banner - Server: Microsoft-IIS/6.0
443	tcp	https	Banner - Server: Microsoft-IIS/6.0

192.168.235.58 : Vulnerabilities

Mail Relaying Allowed

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0512, CVE-2002-1278, CVE-2003-0285

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 10262
BID: 6118, 7580, 8196

Issue Description:

The remote SMTP server seems to allow the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

Suggestions:

Configure your SMTP server so that it can't be used as a relay any more.

Microsoft Outlook Web Access 2003 vulnerable to URL Injection.

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2005-0420

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 17636
Bugtraq ID: 12459
CVE ID: 2005-0420
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0001.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-07/0504.html
Other Advisory URL: http://exploitlabs.com/files/advisories/EXPL-A-2005-001-owa.txt
Secunia Advisory ID: 14144
Security Tracker: 1013086

192.168.235.58 : Vulnerabilities

Issue Description:

The remote host is running Microsoft Outlook Web Access 2003.
Due to a lack of santization of the user input.

The remote version of this software is vulnerable to URL injection which can be exploited to redirect a user to a different, unauthorized web server after authenticating to OWA. This unauthorized site could be used to capture sensitive information by appearing to be part of the web application.

Suggestions:

The vendor has addressed this issue in Exchange 2007. Contact the vendor for details.

Microsoft Outlook Web Access 2003 vulnerable to URL Injection.

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2005-0420

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 17636
Bugtraq ID: 12459
CVE ID: 2005-0420
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0001.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-07/0504.html
Other Advisory URL: http://exploitlabs.com/files/advisories/EXPL-A-2005-001-owa.txt
Secunia Advisory ID: 14144
Security Tracker: 1013086

Issue Description:

The remote host is running Microsoft Outlook Web Access 2003.
Due to a lack of santization of the user input.

The remote version of this software is vulnerable to URL injection which can be exploited to redirect a user to a different, unauthorized web server after authenticating to OWA. This unauthorized site could be used to capture sensitive information by appearing to be part of the web application.

Suggestions:

The vendor has addressed this issue in Exchange 2007. Contact the vendor for details.

192.168.235.58 : Vulnerabilities

HTTP Basic Logins Sent Over Unencrypted Connection

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95243

Issue Description:

Any area of a web application that possibly contains sensitive information or access to privileged functionality such as remote site administration functionality should utilize SSL or another form of encryption to prevent login information from being sniffed or otherwise intercepted or stolen.

An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack, possibly leading to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.

Raw Scanner Output:

http://192.168.235.58:80/public/

Suggestions:

Recommendations include ensuring that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted.

SSL Certificate Expiry

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 15901

192.168.235.58 : Vulnerabilities

Issue Description:

It appears that the SSL certificate used by this server has already expired, or will shortly expire. This will cause error messages to be generated by the user's browser and decreases the level of trust users can have in the authenticity of the server.

The greatest risk in expired SSL certs is that the client is not able to validate the server. If the server was to be spoofed the client will unknowingly be communicating with a malicious server.

Suggestions:

Apply for a new certificate from your preferred Certificate Authority or PKI.

FTP Supports Clear Text Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 34324

Issue Description:

The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

Suggestions:

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.

Comments:

Created On: 2009-12-22 10:46:34
Moderated to impact: medium
This issue rating was increased due to the risks associated with clear text communications across open networks such as the Internet.

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

192.168.235.58 : Vulnerabilities

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95186

Issue Description:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

Raw Scanner Output:

/exchweb/bin/auth/owalogon.asp

Suggestions:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Firewall Enabled

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 27576

Issue Description:

The remote host is behind a firewall.

Based on the responses obtained by the TCP scanner, it was possible to determine that the remote host seems to be protected by a firewall.

192.168.235.58 : Vulnerabilities

Suggestions:

Informational plugin.

AutoComplete Attribute Not Disabled for Password in Form Based Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95186

Issue Description:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

The passwords entered by one user could be stored by the browser and retrieved for another user using the browser.

Raw Scanner Output:

/exchweb/bin/auth/owalogon.asp

Suggestions:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Impact: Level 2 - Medium

CVSS Score: 6.4

CVE Reference: CVE-2009-3555

Port/Protocol: 443/TCP

192.168.235.58 : Vulnerabilities

Other References:

Nessus NASL ID : 42880
http://extendedsubset.com/?p=8
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.kb.cert.org/vuls/id/120541
http://www.g-sec.lu/practicaltls.pdf
https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt
BID:36935
OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974

Issue Description:

The remote service allows renegotiation of TLS / SSL connections.

Suggestions:

No suggestion at this time

SSL Certificate - Signature Verification Failed Vulnerability

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95242

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

192.168.235.58 : Vulnerabilities

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

FTP Server type and version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 10092

Issue Description:

The login banner gives potential attackers additional information about the system they are attacking.

Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
The remote FTP banner is :
220 Microsoft FTP Service

Suggestions:

Informational plugin.

Web Server Uses Basic Authentication

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 34850

192.168.235.58 : Vulnerabilities

Issue Description:

The remote web server contains web pages that are protected by 'Basic' authentication over plain text.
An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Raw Scanner Output:

Plugin output :
The following pages are protected.
/public:/ realm="192.168.235.58"
/exchange:/ realm="192.168.235.58"

Suggestions:

Ensure that HTTP authentication is transmitted over HTTPS.

CN does not match hostname

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 95137

SMTP Server type and version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 10263

Issue Description:

The SMTP Server's type and version can be detected by connecting to the server and processing the buffer received.

192.168.235.58 : Vulnerabilities

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
Remote SMTP server banner :
220 cook.asvtestbed.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0
ready at Mon, 7 Dec 2009 15:13:42 -0500

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port through TLSv1.

Suggestions:

Informational plugin.

TCP timestamps

Impact: Level 1 - Low

192.168.235.58 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

SSL Certificate Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10863

Issue Description:

The scanner was able to determine what SSL ciphers are supported by the server.

The use of weak ciphers may lead to the compromise of data in transit.

Raw Scanner Output:

Plugin output :
Subject Name:
Country: CA
State/Province: Ontario
Locality: Ottawa
Organization: EWA-Canada

192.168.235.58 : Vulnerabilities

Organization Unit: ASVV Lab
Common Name: cook
Issuer Name:
Country: CA
State/Province: Ontario
Locality: Ottawa
Organization: EWA-Canada
Common Name: CA
Email Address: noc@ewa-canada.com
Serial Number: 00 C5 CA 04 BD 08 09 F2 01
Version: 1
Signature Algorithm: SHA-1 With RSA Encryption
Not Valid Before: Dec 04 18:14:15 2008 GMT
Not Valid After: Dec 04 18:14:15 2009 GMT
Public Key Info:
Algorithm: RSA Encryption
Public Key: 00 C2 E5 8A E7 8C 0F 42 B5 1C CC D5 50 99 25 65 54 73 6E 76
B7 CF 78 CB 63 AA 44 17 8D C1 E9 C3 7F 06 3C 88 30 A6 89 C2
D8 F3 CD 35 9B 03 82 C7 CE 7F 85 12 5C DB 37 E8 9A 4F C7 4F
3F 18 DF 70 E2 7F DC 5C 59 72 09 B7 93 4F 13 F7 E1 49 14 19
BD 05 9A 7B A7 0A C8 2C EA 71 62 14 49 25 6C 93 A3 70 B4 FE
D4 0A 9A 66 93 96 44 8F C4 83 3F FD 74 71 81 0F 6A 94 06 85
6D 0C 83 84 1A 37 7F 52 AB
Exponent: 01 00 01
Signature: 00 6D 68 E7 1E 73 EA 5B 01 B0 4D F1 4C 29 68 13 9C 54 D8 2B
8C 1F 26 3D BB 3B 73 5D 60 9B EE D8 86 39 EF 21 3E DC 55 6C
24 52 47 D7 1C 84 6C 4D 11 35 8B 12 5E 1F 8E 8C 01 53 36 FA
DF 81 DC 56 D2 78 07 39 03 C3 D3 54 D3 41 14 84 FC 6C F5 A7
EA CE BE A9 17 5F 48 C9 82 9B 08 DD B7 91 4C C5 5F FB 3A C3
C6 CC 6E FC 7F BA 68 69 79 B5 82 EB 39 BD 6A 42 9C A9 3C 60
19 DF 8B DC FF 0F 2B A7 8F

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 22964

192.168.235.58 : Vulnerabilities

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An FTP server is running on this port.

Suggestions:

Informational plugin.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories require authentication:
/exchange, /public

Suggestions:

It should be verified that no directories found, include sensitive information.

HTTP Type and Version

192.168.235.58 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Microsoft-IIS/6.0

Suggestions:

Informational plugin.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

192.168.235.58 : Vulnerabilities

Raw Scanner Output:

Remote operating system : Microsoft Windows Server 2003
Confidence Level : 75
Method : HTTP
The remote host is running Microsoft Windows Server 2003

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

Reverse NAT/Intercepting Proxy Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.58 : Vulnerabilities

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 31422
http://en.wikipedia.org/wiki/Proxy_server#Intercepting_proxy_server

Issue Description:

Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address.

Based on OS fingerprinting results, it seems that different operating systems are listening on different remote ports. Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.

Suggestions:

Ensure that this setup is authorized by your security policy

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Synopsis :
Some information about the remote HTTP configuration can be extracted.

192.168.235.58 : Vulnerabilities

Description :
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.
Solution :
n/a
Risk factor :
None
Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :
Content-Length: 1433
Content-Type: text/html
Content-Location: http://192.168.235.58/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:1ba4"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 07 Dec 2009 21:06:58 GMT

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

192.168.235.58 : Vulnerabilities

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.58 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.184.186
4.68.110.77
4.68.16.190
4.69.134.121
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.58

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and

192.168.235.58 : Vulnerabilities

Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Synopsis :
Some information about the remote HTTP configuration can be extracted.
Description :
This test gives some information about the remote HTTP protocol - the
version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,
etc...
This test is informational only and does not denote any security
problem.
Solution :
n/a
Risk factor :
None
Plugin output :
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :
Content-Length: 1433
Content-Type: text/html
Content-Location: https://192.168.235.58/iisstart.htm
Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT
Accept-Ranges: bytes
ETag: "06be97f14dac21:1ba4"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 07 Dec 2009 21:06:58 GMT
Connection: close

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

SMTP server fingerprinting

Impact: Level 1 - Low

192.168.235.58 : Vulnerabilities

CVE Reference: CAN-2003-0172

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 11421

Issue Description:

Smtpscan is a SMTP fingerprinting tool. It identifies the remote mail server even if the banners were changed.

Although the banner might have been changed, smtpscan might be able to fingerprint the version number and type.

Raw Scanner Output:

Plugin output :
This server could be fingerprinted as :
Microsoft ESMTP MAIL Service, Version 6.0.3718.0 (Exchange 2003)
Microsoft ESMTP MAIL Service, Version 6.0.3790.1830 (Exchange 2003)

Protected web pages

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 40665

Issue Description:

Some web pages needs authentication.

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :
- Basic is the simplest but the credential are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

192.168.235.58 : Vulnerabilities

Raw Scanner Output:

```
Plugin output :
The following pages are protected by the Basic authentication scheme :
/public
/exchange
```

Suggestions:

Informational plugin

Supported SSL Ciphers Suites

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

```
Nessus NASL ID : 21643
http://www.openssl.org/docs/apps/ciphers.html
```

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Raw Scanner Output:

```
Plugin output :
Here is the list of SSL ciphers supported by the remote server :
  High Strength Ciphers (>= 112-bit key)
    SSLv3
      DES-CBC3-SHA            Kx=RSA      Au=RSA    Enc=3DES(168)
Mac=SHA1
      RC4-MD5                 Kx=RSA      Au=RSA    Enc=RC4(128)
Mac=MD5
      RC4-SHA                 Kx=RSA      Au=RSA    Enc=RC4(128)
Mac=SHA1
The fields above are :
  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
```

192.168.235.58 : Vulnerabilities

{export flag}

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The ICMP timestamps seem to be in little endian format (not in network
format)
The remote clock is synchronized with the local clock.
CVE : CVE-1999-0524

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

HTTP Type and Version

Impact: Level 1 - Low

192.168.235.58 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Microsoft-IIS/6.0

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A TLSv1 server answered on this port.

192.168.235.58 : Vulnerabilities

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SMTP server is running on this port.

Suggestions:

Informational plugin.

192.168.235.58 : Potential Vulnerabilities

MS04-035: Microsoft SMTP Remote Code Execution

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2004-0840

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 15464
Bugtraq ID: 11374
CVE ID: 2004-0840
ISS X-Force ID: 17621
Microsoft Knowledge Base Article: 885881
Microsoft Security Bulletin: MS04-035
Secunia Advisory ID: 12807
Security Tracker: 1011636

Issue Description:

The remote host is running a version of Microsoft SMTP server which is vulnerable to a buffer overflow issue.

An attacker may exploit this flaw to execute arbitrary commands on the remote host with the privileges of the SMTP server process.

Suggestions:

Microsoft has released a patch to fix this vulnerability. More information can be found at:
http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx

MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check)

Impact: Level 5 - Urgent

CVE Reference: CAN-2004-0791, CAN-2004-1060, CVE-2004-0230, CVE-2004-0790, CVE-2004-0791, CVE-2004-1060, CVE-2005-0048, CVE-2005-0688, CVE-2004-0791

Port/Protocol: 0/TCP

192.168.235.58 : Potential Vulnerabilities

Other References:

Nessus NASL ID : 18028

Issue Description:

Arbitrary code can be executed on the remote host due to a flaw in the TCP/IP stack.

The remote host runs a version of Windows that has a flaw in its
TCP/IP stack.
The flaw may allow an attacker to execute arbitrary code with SYSTEM privileges on the remote host or to perform a denial of service attack against the remote host.
Proof of concept code is available to perform a denial of service
attack against a vulnerable system.

Suggestions:

Microsoft has released a set of patches for Windows 2000, XP and
2003 : http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx

Windows Service Pack Level Appears Outdated

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11874
http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/default.mspx

Issue Description:

The Service Pack Level of the remote Windows server appears to be lower than the current service pack level.
The 'Scan Results' section will indicate what service pack is installed.

New vulnerabilities may have been released after the service pack installed was released. The latest service pack should be installed to reduce the risk of new vulnerabilities on the system.

Suggestions:

Ensure that the server is running the latest stable Windows Service Pack.

192.168.235.58 : Potential Vulnerabilities

Please note also that Windows NT4.0 is no longer being supported by Microsoft. NT4.0 users are encouraged to upgrade to Windows 2000 or Windows 2003.

Windows Service Pack Level Appears Outdated

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 443/TCP

Other References:

Nessus NASL ID : 11874
http://www.microsoft.com/technet/prodtechnol/windows2000serv/downloads/default.mspx

Issue Description:

The Service Pack Level of the remote Windows server appears to be lower than the current service pack level.
The 'Scan Results' section will indicate what service pack is installed.

New vulnerabilities may have been released after the service pack installed was released. The latest service pack should be installed to reduce the risk of new vulnerabilities on the system.

Suggestions:

Ensure that the server is running the latest stable Windows Service Pack.
Please note also that Windows NT4.0 is no longer being supported by Microsoft. NT4.0 users are encouraged to upgrade to Windows 2000 or Windows 2003.

ICMP Based TCP Reset Denial of Service Vulnerability

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: CAN-2004-1060, CVE-2004-0790, CAN-2004-0791

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 95230

192.168.235.58 : Potential Vulnerabilities

BugTraq ID: 13124

Issue Description:

The target host is vulnerable to a denial of service condition. The TCP stack present on the host allows an ICMP hard-error packet to reset an established TCP connection that the packet identifies. An example ICMP hard error (defined in the IETF RFCs) is the ICMP message "fragmentation required, but Do-Not-Fragment bit is set".

Since ICMP packets can be spoofed, attackers can exploit this issue by guessing the IP address and port numbers of a TCP connection established on the host, and then resetting these connections simply by sending an ICMP hard-error packet.

Suggestions:

HP has released an updated advisory HPSBUX01164 to address this issue.
IBM has released an advisory IBM-04-12-2005 and the following APARs to address the issue:
AIX Version 5.1: IY70028
AIX Version 5.2: IY70027
AIX Version 5.3: IY70026
Microsoft Security Bulletin MS05-019.
Sun has released an updated advisory Alert ID: 101658 and reports that Sun Solaris versions 7, 8, 9, and 10 are prone to this issue.
Symantec has released an advisory SYM05-008
Cisco has released an advisory 64520 and fixes to address these vulnerabilities.
A workaround is to block ICMP hard-error packets using a firewall.

192.168.235.59 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
web06
OS - OS Name
Windows 5.2
PORT - Port/Protocol/Service/Banner Information
3306/tcp(mysql) none
PORT - Port/Protocol/Service/Banner Information
80/tcp(www) Apache 2.2.3 (Win32) DAV 2 mod_ssl 2.2.3 OpenSSL 0.9.8c mod_autoindex_color PHP 5.1.6

Open Ports

Port	Protocol	Service	Comment
80	tcp	http	Banner - Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c mod_autoindex_color PHP/5.1.6
123	udp	ntp	Service - NTP
137	udp	netbios-ns	Service - netbios-ns
138	udp	netbios-dgm	Service - netbios-dgm
445	udp	microsoft-ds	Service - microsoft-ds
500	udp	isakmp	Service - isakmp
1026	udp	cap	Unknown
3306	tcp	mysql	Banner - 5.0.24a-community-nt

192.168.235.59 : Vulnerabilities

SQL Injection (confirmed)

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95106
http://products.spidynamics.com/asclabs/sql_injection.pdf
http://products.spidynamics.com/asclabs/blind_sql_injection.pdf
http://msdn.microsoft.com/msdnmag/issues/04/09/SQLInjection/default.aspx
http://support.microsoft.com/default.aspx?scid=kb;en-us;302570
http://www.sqlsecurity.com/DesktopDefault.aspx
http://www.owasp.org/index.php/SQL_Injection

Issue Description:

Critical SQL Injection vulnerabilities have been identified in the web application.
SQL injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept. The exploitation takes place in any application parameter that influences a database query. Examples include parameters within the url itself, post data, or cookie values. If successful, SQL Injection can give an attacker access to back-end database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the server hosting the database.

Fundamentally, SQL Injection is an attack upon the web application, not the web server or the operating system itself. As the name implies, SQL Injection is the act of adding an unexpected SQL commands to a query, thereby manipulating the database in ways unintended by the database administrator or developer. When successful, data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications. In certain circumstances, SQL Injection can be utilized to take complete control of a system.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=14%09and%09(se
lect%09count(*)%09from%09sp
http://192.168.235.59/recipe/recipe/login.php:{Username,Password}

Suggestions:

Use the following recommendations to code web applications that are not susceptible to SQL Injection attacks.
i) Parametrized Queries: SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is to separate the logic of a query from

its data. This will prevent commands inserted from user input from being executed. The downside of this approach is that it can have an impact on performance, albeit slight, and that each query on the site must be structured in this method for it to be completely effective. If one query is inadvertently bypassed, that could be enough to leave the application vulnerable to SQL Injection.
ii) Validate input: The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format. The best method of doing this is via "white listing". This is defined as only accepting specific account numbers or specific account types for those relevant fields, or only accepting integers or letters of the English alphabet for others. Many developers will try to validate input by "black listing" characters, or "escaping" them. Basically, this entails rejecting known bad data, such as a single quotation mark, by placing an "escape" character in front of it so that the item that follows will be treated as a literal value. This approach is not as effective as white listing because it is impossible to know all forms of bad data ahead of time.

SQL Injection Confirmed (No Data Extraction)

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95108
http://products.spidynamics.com/asclabs/sql_injection.pdf
http://products.spidynamics.com/asclabs/blind_sql_injection.pdf
http://msdn.microsoft.com/msdnmag/issues/04/09/SQLInjection/default.aspx
http://support.microsoft.com/default.aspx?scid=kb;en-us;302570
http://www.sqlsecurity.com/DesktopDefault.aspx
http://www.owasp.org/index.php/SQL_Injection

Issue Description:

Critical SQL Injection vulnerabilities have been identified in the web application. SQL Injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept. This can be exploited in any application parameter that influences a database query. Examples include parameters within the url itself, post data, or cookie values. If successful, SQL Injection can give an attacker access to back-end database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the server hosting the database.

Fundamentally, SQL Injection is an attack upon the web application, not the web server or the operating system itself. As the name implies, SQL Injection is the act of adding an unexpected SQL commands to a query, thereby manipulating the database in ways unintended by the database administrator or developer. When successful, data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications. In certain circumstances, SQL Injection can be utilized to take complete control of a system.

192.168.235.59 : Vulnerabilities

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/login.php?Username=llllll'%09and%09(
select%09count(*)%09from%09

Suggestions:

There are two ways to mitigate the possibility of SQL Injection attacks:
i) Parametrized Queries: SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is thereby to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed. The downside of this approach is that it can have an impact on performance, albeit slight, and that each query on the site must be structured in this method for it to be completely effective. If one query is inadvertently bypassed, that could be enough to leave the application vulnerable to SQL Injection.
ii) Validate input: The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format. The best method of doing this is via "white listing". This is defined as only accepting specific account numbers or specific account types for those relevant fields, or only accepting integers or letters of the English alphabet for others. Many developers will try to validate input by "black listing" characters, or "escaping" them. Basically, this entails rejecting known bad data, such as a single quotation mark, by placing an "escape" character in front of it so that the item that follows will be treated as a literal value. This approach is not as effective as white listing because it is impossible to know all forms of bad data ahead of time.

Blind SQL Injection (confirmed)

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95244

Issue Description:

SQL injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept, and can be exploited in any application parameter that influences a database query. Examples include parameters within the url itself, post data, or cookie values. Normal SQL Injection attacks depend in a large measure on an attacker reverse engineering portions of the original SQL query using information gained from error messages. However, your application can still be susceptible to Blind SQL injection even if no error message is displayed. If successful, SQL Injection can give an attacker access to backend database contents, the ability to remotely execute system commands, or in some circumstances the means to take control of the server hosting the database.

Fundamentally, SQL Injection is an attack upon the web application, not the web server or the operating

system itself. As the name implies, SQL Injection is the act of adding an unexpected SQL commands to a query, thereby manipulating the database in ways unintended by the database administrator or developer. When successful, data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications. In certain circumstances, SQL Injection can be utilized to take complete control of a system.

Raw Scanner Output:

http://192.168.235.59:80/recipe/form_drafts/category_edit.php

Suggestions:

Recommendations include employing a layered approach to security that includes utilizing parameterized queries when accepting user input, ensuring that only expected data is accepted by an application, and hardening the database server to prevent data from being accessed inappropriately.

Database Server Error Message

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95104
Find instructions on turning off detailed error messaging in IIS at this link:
http://support.microsoft.com/kb/294807
Find information on suppressing error messages on an Apache server at the following locations:
Apache HTTP Server Version 1.3 Custom Error Responses
Apache HTTP Server Version 2.0 Custom Error Responses

Issue Description:

Critical database server error message vulnerabilities were identified in the web application. This indicates that an unhandled exception was generated in your web application code. When successfully exploited, an attacker can gain unauthorized access to the database by using the information recovered from seemingly innocuous error messages. The error messages can pinpoint flaws in the web application and reveal additional avenues of attack.

The way the error messages were created will drive the severity of the vulnerability. In most cases, it will be the result of the web application attempting to use an invalid client-supplied argument in a SQL statement. This means SQL injection is possible. If the injection is successful an attacker will at least be able to read the contents of the entire database arbitrarily. Depending on the database server and the SQL statement, deleting, updating and adding records and executing arbitrary commands may also be possible. If a software bug or bug is responsible for triggering the error, the potential impact will

vary, depending on the circumstances. The location of the application that caused the error can be useful in facilitating other kinds of attacks.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/login.php?Username='&Password=llll&submit=Login
http://192.168.235.59:80/recipe/recipe/login.php?Username=llllll&Password='&submit=Login
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%0aA:B
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%2500
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%250a
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=/%2A
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%2A
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=/
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%00/etc/passwd%00
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%2f%2c%25ENV%2c%2f
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%0d%0aInjectedHeader:%20InjectedValue
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=())[]]{}}
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=,`@^*$#
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId="
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId='
http://192.168.235.59:80/recipe/recipe/recipe_view.php?intId=%00
http://192.168.235.59:80/recipe/recipe/login.php?Username=%27+or+1%3D1--&Password=&submit=Login
http://192.168.235.59:80/recipe/recipe/login.php?Username=admin%27*%2F&Password=--&submit=Login
http://192.168.235.59:80/recipe/recipe/login.php?Username=%27%5C%2F%5C%2F%5C%2F%5C%2F&Password=%5C%5C%
http://192.168.235.59/recipe/recipe/user_add.php
http://192.168.235.59/recipe/recipe/add.php

Suggestions:

From a development perspective, the best method of limiting vulnerabilities arising from error message displays, is to adopt secure programming techniques that will prevent an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.
- Stringently define the data type that the application will accept.
- Validate input in such a way to filter out improper characters.
- Do not display error messages in a way that could be utilized in orchestrating an attack.
- Define the allowed set of characters.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

192.168.235.59 : Vulnerabilities

Cross-Site Scripting

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95105
http://products.spidynamics.com/asclabs/cross-site_scripting.pdf
http://www.owasp.org/documentation/topten/a4.html
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q252985
http://www.microsoft.com/downloads/details.aspx?familyid=9a2b9c92-7ad9-496c-9a89-af08de2e5982&displaylang=en
http://www.cert.org/advisories/CA-2000-02.html
http://httpd.apache.org/info/css-security/apache_specific.html
http://channels.netscape.com/ns/browsers/security.jsp
http://www.securityfocus.com/infocus/1768

Issue Description:

Cross-Site Scripting (XSS) vulnerabilities were verified whilst executing code on the web application. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated. This will allow an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site.

XSS can generally be subdivided into two categories:
i) stored and
ii) reflected attacks.
The main difference between the two is in how the payload arrives at the server. Stored attacks payloads are stored on the target server, such as in a database, or via a submission to a bulletin board or visitor log. The victim will retrieve and execute the attack code in his browser when a request is made for the stored information.
Reflected attacks come from somewhere else. This happens when user input from a web client is immediately included via server-side scripts in a dynamically generated web page. Utilizing social engineering techniques , an attacker can trick a victim, such as through a malicious link or "rigged" form, to submit information which will be altered to include attack code and then sent to the legitimate server. The injected code is then reflected back to the user's browser which executes it because it came from a trusted server. The implication of each kind of attack is the same.
The main problems associated with successful Cross-Site Scripting attacks are:
i) Account hijacking - An attacker can hijack the user's session before the session cookie expires and take actions with the privileges of the user who accessed the URL, such as issuing database queries and viewing the results.
ii) Malicious script execution - Users can unknowingly execute JavaScript, VBScript, ActiveX, HTML, or even Flash content that has been inserted into a dynamically generated page by an attacker.
iii) Worm propagation - With Ajax applications, XSS can propagate somewhat like a virus. The XSS payload

can autonomously inject itself into pages, and easily re-inject the same host with more XSS, all of which can be done with no hard refresh. Thus, XSS can send multiple requests using complex HTTP methods to propagate itself invisibly to the user.
iv) Information theft - Through redirection and fake sites, attackers can connect users to a malicious server of the attacker's choice and capture any information entered by the user.
v) Denial of Service - Often by utilizing malformed display requests on sites that contain a Cross-Site Scripting vulnerability, attackers can cause a denial of service condition to occur by causing the host site to query itself repeatedly.
vi) Browser Redirection - On certain types of sites that use frames, a user can be made to think that he is in fact on the original site when he has been redirected to a malicious one, since the URL in the browser's address bar will remains the same. This is because the entire page isn't being redirected, just the frame in which the JavaScript is being executed.
vii) Manipulation of user settings - Attackers can change user settings for nefarious purposes.

Raw Scanner Output:

http://192.168.235.59:80/recipe/form_drafts/cc_year_edit.php?intId=1"><scri
pt>alert(25457)</script>
http://192.168.235.59:80/recipe/recipe/recipe_list.php?intId=3"><script>ale
rt(53252)</script>
http://192.168.235.59:80/recipe/recipe/recipe_search.php
http://192.168.235.59/recipe/recipe/guestbook_add.php?name=&email=&message=
<script>alert(1)</script>
http://192.168.235.59/recipe/assets/php/_core/calendar.php?intTimestamp=123
5203200&strFormId=<script>alert(1)</script>&strId=
http://192.168.235.59/recipe/recipe/cat.php/"><script>alert(1)</script>
http://192.168.235.59/recipe/recipe/index.php/"><script>alert(1)</script>
http://192.168.235.59/recipe/recipe/user_add.php/"><script>alert(1)</script
>
http://192.168.235.59/recipe/recipe/comments_add.php/"><script>alert(1)</sc
ript>
http://192.168.235.59/recipe/recipe/profile.php/"><script>alert(1)</script>
http://192.168.235.59/recipe/assets/php/_core/error_already_rendered_page.p
hp:strHtml

Suggestions:

Cross-Site Scripting attacks can be avoided by carefully validating all input, and properly encoding all output. Validation can be done using standard ASP.NET Validation controls, or directly in your code. Always use the most stringent pattern possible.
Encoding of output ensures that any scriptable content is properly encoded for HTML before being sent to the client. This is done with the function HttpUtility.HtmlEncode, as shown in the following Label control sample:
Label2.Text = HttpUtility.HtmlEncode(input)
Be sure to consider all paths that user input takes through your application. For instance, if data is entered by the user, stored in a database, and then redisplayed later, you must make sure it is properly encoded each time it is retrieved. If you must allow free-format text input, such as in a message board, and you wish to allow some HTML formatting to be used, you can handle this safely by explicitly allowing only a small list of safe tags.

192.168.235.59 : Vulnerabilities

Unencrypted Login Form

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95114
http://www.kb.cert.org/vuls/id/466433

Issue Description:

An unencrypted login form has been discovered.
Any area of a web application that possibly contains sensitive information or access to privileged functionality such as remote site administration functionality should utilize SSL or another form of encryption to prevent login information from being sniffed or otherwise intercepted or stolen.

An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack. This could lead to the impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/login.php

Suggestions:

Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted.
A page containing a login form should be sent over SSL as well as the Action of the form. This will prevent Man-in-the-Middle attacks on the login form.

Logins Sent Over Unencrypted Connection

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

192.168.235.59 : Vulnerabilities

Nessus NASL ID : 95109

Issue Description:

Login credentials are currently sent in clear text. Any area of a web application that possibly contains sensitive information or access to privileged functionality should utilize SSL or another form of encryption to prevent login information from being sniffed or otherwise intercepted or stolen.

An attacker who exploits this design vulnerability would be able to utilize the information to escalate their method of attack. This could possibly lead to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/login.php

Suggestions:

Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data from being intercepted.

PHP Nested Array Denial Of Service

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95245

Issue Description:

A PHP user data handling denial of service vulnerability has been detected. An attacker can make a request to any PHP page with a deeply nested array variable, which causes PHP to crash when destroying the array. The crashing of PHP can potentially have server-wide effects as well, depending on the web server hosting PHP.

An attack can cause momentary excessive resource consumption on the web server and abnormal web application termination. Depending on the web server software and/or configuration, it may also lead to a full web server crash.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/index.php

192.168.235.59 : Vulnerabilities

Suggestions:

Recommendations include upgrading to a fixed version of PHP.

Password in Query Data

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95110

Issue Description:

A password was found in the query string of a GET request.

Leaving login information in a query string makes it easy for an attacker to see and tamper with login values.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/login.php?Username=llllll&Password=l
lll&submit=Login

Suggestions:

The process to login should be changed to allow for login information to be sent with POST data over an encrypted connection.

UDP packets with source port of 53 bypass firewall rules

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-1473

Port/Protocol: 0/UDP

Other References:

192.168.235.59 : Vulnerabilities

Nessus NASL ID : 11580
Bugtraq ID: 11237
CERT VU: 329230
CVE ID: 2004-1473
ISS X-Force ID: 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 12635
Security Tracker: 1011388, 1011389
Vendor Specific Advisory URL:
http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor URL: http://www.symantec.com/

Issue Description:

It is possible to by-pass the rules of the remote firewall by sending UDP packets with a source port equal to 53.

An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall.

Suggestions:

Review your firewall rules policy and ensure that your firewall is stateful (tracks the state of allowed connections).

Directory Listing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95115
Apache:
http://httpd.apache.org/docs/misc/security_tips.html
http://www.w3.org/Security/faq/wwwsf3.html
http://linux.omnipotent.net/article.php?article_id=3667
IIS:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/iis/default.mspx
Netscape:
http://www.belk.com/manual/ag/esaccess.htm

192.168.235.59 : Vulnerabilities

Issue Description:

A serious Directory Listing vulnerability was discovered within the web application.
Risks associated with an attacker discovering a Directory Listing, which is a complete index of all of the resources located in that directory, result from the fact that files that should remain hidden, such as data files, backed-up source code, or applications in development, may then be visible. The specific risks depend upon the specific files that are listed and accessible.

Risks associated with an attacker discovering a Directory Listing on your application server depend upon what type of directory is discovered, and what types of files are contained within it.
The primary threat from an accessible Directory Listing is that hidden files such as data files, source code, or applications under development will then be visible to a potential attacker. In addition to accessing files containing sensitive information, other risks include an attacker utilizing the information discovered in that directory to perform other types of attacks.

Raw Scanner Output:

http://192.168.235.59:80/icons/
http://192.168.235.59:80/recipe/assets/js/_core/
http://192.168.235.59:80/recipe/assets/
http://192.168.235.59:80/recipe/assets/js/
http://192.168.235.59:80/recipe/assets/css/
http://192.168.235.59:80/recipe/assets/images/
http://192.168.235.59:80/recipe/recipe/category_images/
http://192.168.235.59:80/icons/small/

Suggestions:

Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application.
i) Restrict access to important files or directories only to those who actually need it.
ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.

Script Name/Path Parameter Cross-Site Scripting

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95248

192.168.235.59 : Vulnerabilities

Issue Description:

Cross-Site Scripting was discovered due to the web page displaying the original URL without first filtering it. Cross-Site Scripting occurs when dynamically generated web pages display user input, such as the original URL, program name or path, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. If successful, Cross-Site Scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on end user systems.

Cross-Site Scripting happens when user input from a web client is immediately included via server-side scripts in a dynamically generated web page. Via social engineering, an attacker can trick a victim, such as through a malicious link or "rigged" form, to submit information which will be altered to include attack code and then sent to the legitimate server. The injected code is then reflected back to the user's browser which executes it because it came from a trusted server.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/index.php/a<script>alert(097531)</sc
ript>

Suggestions:

Recommendations include modifying source code to properly validate input parameters or updating to a fixed version of the application.

Possible File Upload Capability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95249

Issue Description:

An indicator of file upload capability was found. File upload capability allows a web user to send a file from his or her computer to the webserver. If the web application that receives the file does not carefully examine it for malicious content, an attacker may be able to use file uploads to execute arbitrary commands on the server.

The exact implications depend upon the nature of the files an attacker would be able to upload. Implications range from unauthorized content publishing to aid in phising attacks, all the way to full

192.168.235.59 : Vulnerabilities

compromise of the web server.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/add.php

Suggestions:

Recommendations include adopting a strict file upload policy that prevents malicious material from being uploaded via sanitization and filtering.

PHP Version Information Disclosure

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95247

Issue Description:

A remote user can determine the version of PHP installed on the system by using an easter egg placed by the PHP developers.

Information disclosure reveals sensitive information about a system or web application to an attacker. An attacker can use this information to learn more about a system when attempting to gain unauthorized access.

Raw Scanner Output:

http://192.168.235.59:80/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

Suggestions:

Recommendations include setting expose_php to Off in your php.ini configuration file.

HTTP TRACE/TRACK Methods Supported

Impact: Level 3 - High

CVSS Score: 4.3

192.168.235.59 : Vulnerabilities

CVE Reference: CVE-2004-2320, CVE-2005-3398, CVE-2005-3498, CVE-2007-3008

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11213
Bugtraq ID: 11604, 9561, 9506
CERT VU: 867593
CVE ID: 2005-3398, 2005-3498, 2004-2320
ISS X-Force ID: 11149, 11237, 14959
Mail List Post: http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html
Nikto Item ID: 1249, 1250
Other Advisory URL: http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
Other Advisory URL: http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
Other Advisory URL: http://en.wikipedia.org/wiki/Cross-site_tracing
Other Advisory URL: http://dev2dev.bea.com/pub/advisory/68
Related OSVDB ID: 5648, 3726
Secunia Advisory ID: 17334, 21802, 10726, 32977
Security Tracker: 1015112, 102016, 1015134, 1008866
Snort Signature ID: 2056
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1
Vendor Specific Advisory URL:
ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir5.10_docs_relnotes.pdf
Vendor Specific Advisory URL:
http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_48.00.jsp
Vendor Specific News/Changelog Entry:
https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/install/v61.Readme.html#MH01128
Vendor URL:
http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/resources/index.html
Vendor URL: http://www.bea.com
http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp;

Issue Description:

Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick a legitimate web user into disclosing their credentials.

Suggestions:

If you are using Apache, add the following lines for each virtual host in your configuration file:;;
RewriteEngine on;
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK);
RewriteRule .* - [F];;
If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

192.168.235.59 : Vulnerabilities

Exception Error Message

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95246

Issue Description:

Unhandled exceptions are circumstances in which the application has received user input that it did not expect and doesn't know how to deal with. In many cases, an attacker can leverage the conditions that cause these errors in order to gain unauthorized access to the system.

Exception error messages may contain the location of the file in which the offending function is located. This may disclose the webroot's absolute path as well as give the attacker the location of application include files or configuration information. It may even disclose the portion of code that failed. In most cases, it will be the result of the web application attempting to use an invalid client-supplied argument in a SQL statement, which means that SQL injection will be possible. If so, an attacker will at least be able to read the contents of the entire database arbitrarily. Depending on the database server and the SQL statement, deleting, updating and adding records and executing arbitrary commands may also be possible. If a software bug or bug is responsible for triggering the error, the potential impact will vary, depending on the circumstances. The location of the application that caused the error can be useful in facilitating other kinds of attacks. If the file is a hidden or include file, the attacker may be able to gain more information about the mechanics of the web application, possibly even the source code. Application source code is likely to contain usernames, passwords, database connection strings and aids the attacker greatly in discovering new vulnerabilities.

Raw Scanner Output:

http://192.168.235.59:80/recipe/recipe/add.php
http://192.168.235.59:80/recipe/recipe/add.php

Suggestions:

Recommendations include designing and adding consistent error-handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

NetBIOS Name Service Reply Information Leakage

192.168.235.59 : Vulnerabilities

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CAN-2003-0661

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 11830
Microsoft: http://www.microsoft.com/technet/security/bulletin/ms03-034.asp
Bugtraq: http://www.securityfocus.com/bid/8532

Issue Description:

The remote host is running a version of the NetBT name
service which suffers from a memory disclosure problem. An attacker may send a special packet to the
remote NetBT name
service, and the reply will contain random arbitrary data from the remote host memory. This arbitrary
data may be a fragment from the web page the remote user is viewing, or something more serious like a POP
password or anything else. An attacker may use this flaw to continuously 'poll' the content of the memory
of the remote host and might be able to obtain sensitive
information.

A weakness has been reported in NetBIOS on Microsoft Windows operating systems that may enable remote
attackers to gain access to potentially sensitive information. In particular, the NetBIOS Name Service
may leak random memory contents when replying to NetBT Name Service requests.

Suggestions:

Download patch from http://www.microsoft.com/technet/security/bulletin/ms03-034.asp

Expose_php Set to On in php.ini

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95174

Issue Description:

192.168.235.59 : Vulnerabilities

The scanner found PHP version information in the headers returned by the PHP-enabled target Web server. This likely means that the "expose_php" variable is set to "On" in the "php.ini" configuration file for the Web server.

This allows remote users to easily know that PHP is installed on the Web server. It also provides version information of the PHP installation. This could aid an attacker in launching more targeted attacks in the future.

Raw Scanner Output:

```
GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 HTTP/1.1
Host: 192.168.235.59
Connection: Keep-Alive
HTTP/1.1 200 OK
Date: Tue, 08 Dec 2009 01:45:06 GMT
Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c
mod_autoindex_color PHP/5.1.6
X-Powered-By: PHP/5.1.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff
 color: #000000
}
body, td, th, h1, h2 {font-family: sans-serif
}
pre {margin: 0px
 font-family: monospace
}
a:link {color: #000099
 text-decoration: none
 background-color: #ffffff
}
a:hover {text-decoration: underline
}
table {border-collapse: collapse
}
.center {text-align: center
}
.center table { margin-left: auto
 margin-right: auto
 text-align: left
}
.center th { text-align: center !important
 }
```

192.168.235.59 : Vulnerabilities

```
td, th { border: 1px solid #000000
 font-size: 75%
 vertical-align: baseline
}
h1 {font-size: 150%
}
h2 {font-size: 125%
}
.p {text-align: left
}
.e {background-color: #ccccff
 font-weight: bold
 color: #000000
}
.h {background-color: #9999cc
 font-weight: bold
 color: #000000
}
.v {background-color: #cccccc
 color: #000000
}
.vr {background-color: #cccccc
 text-align: right
 color: #000000
}
img {float: right
 border: 0px
}
hr {width: 600px
 background-color: #cccccc
 border: 0px
 height: 1px
 color: #000000
}
</style>
<title>phpinfo()</title></head>
<body><div class="center">
<h1>PHP Credits</h1>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>PHP Group</th></tr>
<tr><td class="e">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi
Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski,
Jim Winstead, Andrei Zmievski </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Language Design & Concept</th></tr>
---truncated ---
```

Suggestions:

192.168.235.59 : Vulnerabilities

Locate the "php.ini" configuration file on the target host and add this setting to it: "expose_php=Off".
Restart the Web server.

phpMyAdmin Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 17219
http://www.phpmyadmin.net/home_page/index.php

Issue Description:

The remote web server contains a database management application
written in PHP.

The remote host is running phpMyAdmin, a web-based MySQL
administration tool written in PHP.

Suggestions:

Informational plugin.

Web Server Uses Basic Authentication

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 34850

Issue Description:

The remote web server contains web pages that are protected by 'Basic' authentication over plain text.
An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

192.168.235.59 : Vulnerabilities

Raw Scanner Output:

Plugin output :
The following pages are protected.
/xampp:/ realm="xampp user"

Suggestions:

Ensure that HTTP authentication is transmitted over HTTPS.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

192.168.235.59 : Vulnerabilities

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The ICMP timestamps seem to be in little endian format (not in network
format)
The difference between the local and remote clocks is 360 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

192.168.235.59 : Vulnerabilities

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

192.168.235.59 : Vulnerabilities

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.59 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78
213.200.73.121
89.149.187.246
4.68.110.77
4.68.16.254
4.69.134.125
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.59

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

WebDAV Methods Supported

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.59 : Vulnerabilities

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11424
Microsoft:;
http://support.microsoft.com/default.aspx?kbid=241520

Issue Description:

The remote web server has WebDAV methods enabled. World Wide Web Distributed Authoring and Versioning (WebDAV) is an industry standard extension to the HTTP specification allowing users to remotely share resources, such as files, over the HTTP protocol.

Various vulnerabilities have been associated with WebDAV, including:;;
- Directory listings using the PROPFIND and SEARCH methods;
- Buffer overflow in an operating system component (ntdll.dll), exploitable through WebDAV (MS03-007);;
Although these vulnerabilities are not necessarily present on the remote server, WebDAV by virtue of the functionality it provides should not be enabled except if absolutely necessary.

Suggestions:

WebDAV should be removed entirely if not in use.;;
For IIS 4.0 and 5.0 run the IIS Lockdown utility available from Microsoft:;
http://www.microsoft.com/technet/security/tools/locktool.mspx;;
Alternatively, to remove WebDAV on IIS see the following Microsoft Knowledge Base Article:;
http://support.microsoft.com/default.aspx?kbid=241520.;

NetBIOS Hostname Retrieval

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0621

Port/Protocol: 137/UDP

Other References:

Nessus NASL ID : 10150
CVE ID: 1999-0621
ISS X-Force ID: 8516
OVAL ID: 1024
Vendor URL: http://www.microsoft.com/

Issue Description:

192.168.235.59 : Vulnerabilities

The NetBIOS port is open (UDP:137). A remote attacker may use this to gain access to sensitive information such as computer name, workgroup/domain name, currently logged on user name, etc.

Raw Scanner Output:

Plugin output :
The following 4 NetBIOS names have been gathered :
DUBCEK = Computer name
WORKGROUP = Workgroup / Domain name
DUBCEK = File Server Service
WORKGROUP = Browser Service Elections
The remote host has the following MAC address on its adapter :
00:50:56:91:54:42

Suggestions:

The NetBIOS port should only be open to internal networks. Block those ports from outside communication.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c mod_autoindex_color
PHP/5.1.6

Suggestions:

Informational plugin.

192.168.235.59 : Vulnerabilities

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge

192.168.235.59 : Vulnerabilities

about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : Microsoft Windows Server 2003
Confidence Level : 70
Method : SinFP
The remote host is running Microsoft Windows Server 2003

Suggestions:

Informational plugin.

VMWare Host

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 20094

Issue Description:

According to the MAC address of its network adapter, the remote host
is a VMWare virtual machine running.

Since it is physically accessible through the network, you should
ensure that its configuration matches the one of your corporate
security policy.

Suggestions:

Informational plugin.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.59 : Vulnerabilities

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/cgi-bin, /webalizer, /error, /icons, /restricted, /server-info, /server-status
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories require authentication:
/xampp
Other references : OWASP:OWASP-CM-006

Suggestions:

It should be verified that no directories found, include sensitive information.

Identify unknown services with GET

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 17975

Issue Description:

This plugin performs service detection.

This plugin is a complement of find_service1.nasl. It sends a GET request to the remaining unknown services and tries to identify them.

192.168.235.59 : Vulnerabilities

Suggestions:

No suggestion at this time

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

Protected web pages

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 40665

Issue Description:

Some web pages needs authentication.

192.168.235.59 : Vulnerabilities

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :
- Basic is the simplest but the credential are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

Raw Scanner Output:

Plugin output :
The following pages are protected by the Basic authentication scheme :
/xampp

Suggestions:

Informational plugin

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes

192.168.235.59 : Vulnerabilities

Options allowed : (Not implemented)
Headers :
Date: Mon, 07 Dec 2009 15:51:22 GMT
Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c
mod_autoindex_color PHP/5.1.6
X-Powered-By: PHP/5.1.6
Location: http://192.168.235.59/recipe/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

192.168.235.59 : Potential Vulnerabilities

PHP < 5.2.9 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2008-5844, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 35750
Bugtraq ID: 33002, 33927
http://news.php.net/php.internals/42762
http://www.php.net/releases/5_2_9.php
http://www.php.net/ChangeLog-5.php#5.2.9

Issue Description:

The remote web server uses a version of PHP that is affected by
multiple flaws.

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such
versions may be affected by several security issues:
- Background color is not correctly validated with a non true
color image in function 'imagerotate()'.(CVE-2008-5498)
- A denial of service condition can be triggered by trying to
extract zip files that contain files with relative paths
in file or directory names.
- Function 'explode()' is affected by an unspecified
vulnerability.
- It may be possible to trigger a segfault by passing a
specially crafted string to function 'json_decode()'.
- Function 'xml_error_string()' is affected by a flaw
which results in messages being off by one.

Suggestions:

Upgrade to PHP version 5.2.9 or later. Please see: http://www.php.net

PHP < 5.2.5 Multiple Vulnerabilities

192.168.235.59 : Potential Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-4783, CVE-2007-4840, CVE-2007-4850, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2007-6039, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 28181
Bugtraq ID: 26403
CVE ID: 2007-5900, 2007-5898, 2007-4887
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0093.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0094.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0096.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0079.html
Other Advisory URL: HPSBUX02308 SSRT080010
Other Advisory URL: HPSBUX02332 SSRT080056
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00006.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-November/000277.html
Other Advisory URL: http://securityreason.com/securityalert/3133
Other Advisory URL: http://www.debian.org/security/2008/dsa-1444
Other Advisory URL: http://www.ubuntu.com/usn/usn-549-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-628-1
Other Advisory URL: http://www.ubuntu.com/usn/USN-720-1
Other Advisory URL: https://issues.rpath.com/browse/RPL-1943
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-June/msg00773.html
Related OSVDB ID: 38681, 38682, 38683, 38684, 38685, 38686, 38680
Secunia Advisory ID: 27648, 27659, 30040, 33939, 27864, 28249, 28658, 30828, 31119, 31124, 31200, 28750, 29420
Security Tracker: 1018934
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific News/Changelog Entry: http://bugs.php.net/bug.php?id=41561
Vendor Specific News/Changelog Entry: http://www.php.net/ChangeLog-5.php#5.2.5
Vendor Specific News/Changelog Entry: http://www.php.net/releases/5_2_5.php
Vendor URL: http://www.php.net/

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.5.

192.168.235.59 : Potential Vulnerabilities

Such versions may be affected by various issues, including but not limited to several buffer overflows.

Suggestions:

Upgrade to PHP version 5.2.5 or later. Please see: http://www.php.net

mod_ssl < 2.8.31

Impact: Level 5 - Urgent

CVE Reference: CVE-2002-0082, CVE-2004-0488, CVE-2004-0700, CVE-2005-2700

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95136

Issue Description:

The server is not running the latest version of mod_ssl.

According to the version number of the Apache banner on the remote host, the mod_ssl version may be vulnerable to a number of flaws, some of which allow code execution.
The issue include the following (depending on the actual version of mod_ssl running on the remote server):
CVE-2002-0082 - Apache HTTP Server mod_ssl i2d_SSL_SESSION Function SSL Client Certificate Overflow
CVE-2004-0488 - Apache HTTP Server mod_ssl ssl_util_uuencode_binary Remote Overflow
CVE-2004-0700 - Apache HTTP Server mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
CVE-2005-2700 - Apache HTTP Server mod_ssl SSLVerifyClient Per-location Context Restriction Bypass

Suggestions:

Upgrade to the latest version of mod_ssl. Please see: http://www.modssl.org/

PHP < 5.2.6 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107,

192.168.235.59 : Potential Vulnerabilities

CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625,
CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 32123
Bugtraq ID: 26426, 27413, 28392, 29009, 33542
http://archives.neohapsis.com/archives/bugtraq/2008-03/0321.html
http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0103.html
http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0107.html
http://www.php.net/releases/5_2_6.php

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.6.

Such versions may be affected by the following issues :
- A stack buffer overflow in FastCGI SAPI.
- An integer overflow in printf().
- An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c.
- A safe_mode bypass in cURL.
- Incomplete handling of multibyte chars inside escapeshellcmd().
- Issues in the bundled PCRE fixed by version 7.6.

Suggestions:

Upgrade to PHP version 5.2.6 or later. Please see: http://www.php.net

PHP < 5.2 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2004-0594, CVE-2004-0595, CVE-2004-0958, CVE-2004-0959,
CVE-2004-1019, CVE-2004-1020, CVE-2004-1065, CVE-2005-0524,
CVE-2005-0525, CVE-2005-3319, CVE-2005-3388, CVE-2005-3389,
CVE-2005-3390, CVE-2005-3883, CVE-2006-0200, CVE-2006-0207,
CVE-2006-0208, CVE-2006-0996, CVE-2006-1014, CVE-2006-1015,
CVE-2006-1017, CVE-2006-1490, CVE-2006-1494, CVE-2006-1549,
CVE-2006-1608, CVE-2006-1990, CVE-2006-1991, CVE-2006-2563,
CVE-2006-2660, CVE-2006-3011, CVE-2006-3016, CVE-2006-3017,
CVE-2006-3018, CVE-2006-4020, CVE-2006-4023, CVE-2006-4433,
CVE-2006-4481, CVE-2006-4482, CVE-2006-4483, CVE-2006-4484,
CVE-2006-4485, CVE-2006-4486, CVE-2006-4625, CVE-2006-4812,

CVE-2006-5178, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1001, CVE-2007-1285, CVE-2007-1376, CVE-2007-1380, CVE-2007-1381, CVE-2007-1396, CVE-2007-1452, CVE-2007-1461, CVE-2007-1484, CVE-2007-1581, CVE-2007-1582, CVE-2007-1583, CVE-2007-1700, CVE-2007-1701, CVE-2007-1710, CVE-2007-1717, CVE-2007-1718, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1883, CVE-2007-1884, CVE-2007-1885, CVE-2007-1887, CVE-2007-1888, CVE-2007-1890, CVE-2007-2509, CVE-2007-2510, CVE-2007-2511, CVE-2007-2727, CVE-2007-2748, CVE-2007-2844, CVE-2007-2872, CVE-2007-3007, CVE-2007-4528, CVE-2007-5128, CVE-2007-5424, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-0754

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 31649
Bugtraq ID: 19933, 20326, 20349, 22805, 22862, 22906, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237
CVE ID: 2006-5465
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-11/0574.html
News Article: http://news.com.com/Apple+Mac+OS+X+patch+plugs+31+vulnerabilities/2100-1002_3-6139117.html
Other Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Nov/0004.html
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200703-21.xml
Other Advisory URL: http://www.hardened-php.net/advisory_132006.138.html
RedHat RHSA: RHSA-2006:0730, RHSA-2006:0736
Related OSVDB ID: 30179, 30178
Secunia Advisory ID: 22653, 22693, 22688, 22685, 22753, 22713, 22759, 22779, 22881, 22929, 23155, 23139, 23247, 24606, 25047
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=304829
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2006.11.28.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-245.htm
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:196
Vendor Specific Advisory URL: http://www.trustix.org/errata/2006/0061/
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-375-1
Vendor Specific Advisory URL: http://www.us.debian.org/security/2006/dsa-1206
Vendor Specific Advisory URL: https://issues.rpath.com/browse/RPL-761
Vendor Specific News/Changelog Entry: http://www.php.net/releases/5_2_0.php
Vendor Specific Solution URL: http://support.veritas.com/docs/285984

192.168.235.59 : Potential Vulnerabilities

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.

Such versions may be affected by several buffer overflows. To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server, or be able to manipulate several variables processed by some PHP functions such as htmlentities().
Other vulnerabilities include:
- PHP Symbolic Link Open_Basedir Bypass Vulnerability (CVE-2006-5178)
- PHP ZendEngine ECalloc Integer Overflow Vulnerability (CVE-2006-4812)
- PHP EXT/Filter FDF Post Filter Bypass Vulnerability (CVE-2007-1452)
- PHP Imap_Mail_Compose() Function Buffer Overflow Vulnerability (CVE-2007-1825)
- PHP Msg_Receive() Memory Allocation Integer Overflow Vulnerability (CVE-2007-1890)
- PHP Shared Memory Functions Resource Verification Arbitrary Code Execution Vulnerability (CVE-2007-1376)
- PHP 5 PHP_Stream_Filter_Create() Function Buffer Overflow Vulnerability (CVE-2007-1824)
- PHP Str_Replace() Integer Overflow Vulnerability (CVE-2007-1885)
- PHP Ini_Restore() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability (CVE-2006-4625)
- PHP Session Data Deserialization Arbitrary Code Execution Vulnerability (CVE-2007-1701)
- PHP PHP_Binary Heap Information Leak Vulnerability (CVE-2007-1380)
- PHP Printf() Function 64bit Casting Multiple Format String Vulnerabilities (CVE-2007-1884)
- PHP sqlite_udf_decode_binary() Function Buffer Overflow Vulnerability (CVE-2007-1887)
- PHP Hash Table Overwrite Arbitrary Code Execution Vulnerability (CVE-2007-1700)

Suggestions:

Upgrade to PHP version 5.2.0 or later. Please see: http://www.php.net

PHP < 5.2.4 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2002-0229, CVE-2007-1413, CVE-2007-2872, CVE-2007-3007, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790, CVE-2007-3799, CVE-2007-3806, CVE-2007-3996, CVE-2007-3997, CVE-2007-3998, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE-2007-4507, CVE-2007-4652, CVE-2007-4657, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-2007-4661, CVE-2007-4662, CVE-2007-4663, CVE-2007-4670, CVE-2007-4782, CVE-2007-4784, CVE-2007-4825, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

192.168.235.59 : Potential Vulnerabilities

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 25971
Bugtraq ID: 24261, 24268, 24661, 24922, 25498, 4026
CVE ID: 2007-2872, 2007-3378, 2007-3806
FrSIRT Advisory: ADV-2007-2061, ADV-2007-3386, ADV-2007-2547
ISS X-Force ID: 35102
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0005.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0341.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0102.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-11/0355.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0079.html
Other Advisory URL: HPSBUX02262 SSRT071447
Other Advisory URL: HPSBUX02308 SSRT080010
Other Advisory URL: HPSBUX02332 SSRT080056
Other Advisory URL: http://blog.php-security.org/archives/86-Chunk_split-Overflow-not-fixed-at-all....html
Other Advisory URL: http://lists.debian.org/debian-security-announce/2008/msg00147.html
Other Advisory URL: http://lists.debian.org/debian-security-announce/2008/msg00156.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00006.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00006.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-October/000269.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-September/000244.html
Other Advisory URL: http://milw0rm.com/exploits/4181
Other Advisory URL: http://securityreason.com/achievement_exploitalert/9
Other Advisory URL: http://securityreason.com/achievement_securityalert/45
Other Advisory URL: http://securityreason.com/securityalert/2831
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.399824
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.482863
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-449.htm
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200710-02.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:187
Other Advisory URL: http://www.openpkg.com/security/advisories/OpenPKG-SA-2007.020.html
Other Advisory URL: http://www.sec-consult.com/291.html
Other Advisory URL: http://www.trustix.org/errata/2007/0023/
Other Advisory URL: http://www.trustix.org/errata/2007/0026/
Other Advisory URL: http://www.ubuntu.com/usn/usn-549-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00321.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00354.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00397.html
RedHat RHSA: RHSA-2007:0890, RHSA-2007:0889, RHSA-2007:0888
Related OSVDB ID: 36084, 36858, 36859, 36861, 36863, 36864, 36865, 36866, 36867, 36870
Secunia Advisory ID: 25456, 26048, 26085, 26231, 26642, 26748, 26802, 26822, 26838, 26871, 26895, 26930, 26967, 27037, 27102, 27110, 27351, 27377, 27545, 27864, 28658, 28750, 29420, 30040, 30040, 30158, 30288
Security Tracker: 1018186

192.168.235.59 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific News/Changelog Entry: http://cvs.php.net/viewvc.cgi/php-src/ext/standard/dir.c?view=log
Vendor Specific News/Changelog Entry: http://www.php.net/ChangeLog-5.php#5.2.4
Vendor Specific News/Changelog Entry: http://www.php.net/releases/4_4_8.php
Vendor Specific News/Changelog Entry: http://www.php.net/releases/5_2_3.php
Vendor Specific News/Changelog Entry: http://www.php.net/releases/5_2_4.php
Vendor URL: http://www.php.net/

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.4.

Such versions may be affected by various issues, including but not limited to several overflows.

Suggestions:

Upgrade to PHP version 5.2.4 or later. Please see: http://www.php.net

PHP < 5.2.1 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2006-6383, CVE-2007-0448, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1001, CVE-2007-1285, CVE-2007-1286, CVE-2007-1375, CVE-2007-1376, CVE-2007-1380, CVE-2007-1383, CVE-2007-1396, CVE-2007-1399, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1460, CVE-2007-1461, CVE-2007-1484, CVE-2007-1522, CVE-2007-1581, CVE-2007-1582, CVE-2007-1583, CVE-2007-1584, CVE-2007-1700, CVE-2007-1701, CVE-2007-1717, CVE-2007-1718, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1883, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1888, CVE-2007-1889, CVE-2007-1890, CVE-2007-1900, CVE-2007-2509, CVE-2007-2510, CVE-2007-2727, CVE-2007-2844, CVE-2007-2872, CVE-2007-3007, CVE-2007-4441, CVE-2007-4586, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

192.168.235.59 : Potential Vulnerabilities

Nessus NASL ID : 24907
Bugtraq ID: 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238
http://www.php.net/releases/5_2_1.php

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.1.

Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.

Suggestions:

Upgrade to PHP version 5.2.1 or later. Please see: http://www.php.net

OpenSSL 0.9 < 0.9.8k

Impact: Level 5 - Urgent

CVSS Score: 7.5

CVE Reference: CVE-1999-0428, CVE-2000-0535, CVE-2001-1141, CVE-2002-0655, CVE-2002-0656, CVE-2002-0657, CVE-2002-0659, CVE-2002-1568, CVE-2003-0078, CVE-2003-0131, CVE-2003-0147, CVE-2003-0543, CVE-2003-0544, CVE-2003-0545, CVE-2003-0851, CVE-2004-0079, CVE-2004-0081, CVE-2004-0112, CVE-2004-0975, CVE-2005-1797, CVE-2005-2946, CVE-2005-2969, CVE-2006-2937, CVE-2006-2940, CVE-2006-3738, CVE-2006-4339, CVE-2006-4343, CVE-2007-3108, CVE-2007-4995, CVE-2007-5135, CVE-2007-5536, CVE-2008-0891, CVE-2008-1678, CVE-2008-5077, CVE-2009-0590, CVE-2009-0591, CVE-2009-0653, CVE-2009-0789, CVE-2009-1377, CVE-2009-1378, CVE-2009-1386, CVE-2009-1387, CVE-2009-2409

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95126

Issue Description:

OpenSSL 0.9 version is older than 0.9.8k.

According to the version number of the OpenSSL banner on the remote host, the OpenSSL 0.9 version may be vulnerable to a number of flaws, some of which allow code execution.

192.168.235.59 : Potential Vulnerabilities

These include the following:
CVE-1999-0428 - OpenSSL Session Reuse Bypass of Client Certificate Access Control
CVE-2000-0535 - OpenSSL and OpenSSH /dev/random Check Failure
CVE-2001-1141 - OpenSSL PRNG Information Disclosure
CVE-2002-0655 - OpenSSL ASCII Integer Overflow
CVE-2002-0656 - OpenSSL SSLv3 Session ID Buffer Overflow, OpenSSL SSLv2 Client Master Key Overflow
CVE-2002-0657 - OpenSSL SSLv3 with Kerberos Master Key Overflow
CVE-2002-0659 - OpenSSL ASN.1 Parser Invalid Encoding DoS
CVE-2002-1568 - OpenSSL SSLv2 Failed Assertion DoS
CVE-2003-0078 - OpenSSL Vaudenay Timing Attack
CVE-2003-0131 - OpenSSL RSA Klima-Pokorny-Rosa Attack
CVE-2003-0147 - OpenSSL Non-RSA Blinding Private Key Disclosure, Multiple SSL/TLS Implementation Non-RSA Blinding Private Key Disclosure
CVE-2003-0543 - OpenSSL ASN.1 Integer Overflow DoS
CVE-2003-0544 - OpenSSL ASN.1 Client Certificate Overflow DoS
CVE-2003-0545 - OpenSSL ASN.1 Client Certificate Double-free
CVE-2003-0851 - OpenSSL ASN.1 Large Recursion DoS
CVE-2004-0079 - OpenSSL SSL/TLS Handshake Null Pointer DoS
CVE-2004-0081 - OpenSSL TLS Infinite Loop DoS
CVE-2004-0112 - OpenSSL Kerberos SSL/TLS Handshake DoS
CVE-2004-0975 - OpenSSL der_chop Script Symlink Arbitrary File Modification
CVE-2005-1797 - Advanced Encryption Standard (AES, aka Rijndael) S-box Lookup Timing Attack
CVE-2005-2946 - OpenSSL Default Algorithm MD5 Weak Digest Encryption
CVE-2005-2969 - OpenSSL SSL_OP_ALL SSL 2.0 Verification Weakness
CVE-2006-2937 - OpenSSL Malformed ASN.1 Structure Resource Consumption DoS
CVE-2006-2940 - OpenSSL Crafted Public Key CPU Consumption DoS
CVE-2006-3738 - OpenSSL SSL_get_shared_ciphers Function Unspecified Remote Overflow
CVE-2006-4339 - OpenSSL RSA Key PKCS #1 v1.5 Signature Forgery
CVE-2006-4343 - OpenSSL SSLv2 get_server_hello Function Remote DoS
CVE-2007-3108 - OpenSSL crypto/bn/bn_mont.c BN_from_montgomery Function Local RSA Key Disclosure
CVE-2007-4995 - OpenSSL DTLS Implementation Unspecified Off-by-one Remote Code Execution
CVE-2007-5135 - OpenSSL SSL_get_shared_ciphers Function Unspecified Remote Overflow
CVE-2007-5536 - OpenSSL on HP-UX Unspecified Local DoS
CVE-2008-0891 - OpenSSL Server Name Extension Data Handling Crafted Packet Remote DoS
CVE-2008-1678 - OpenSSL libssl crypto/comp/c_zlib.c zlib_stateful_init Function Memory Exhaustion Remote DoS
CVE-2008-5077 - OpenSSL EVP_VerifyFinal Function DSA / ECDSA Key Validation Weakness
CVE-2009-0590 - OpenSSL ASN1_STRING_print_ex() Function BMPString / UniversalString Handling DoS
CVE-2009-0591 - OpenSSL CMS_verify() Function Malformed Signed Attribute Content Digest Validity Spoofing
CVE-2009-0653 - OpenSSL Intermediate CA-signed Certificate Basic Constraints Validation Weakness
CVE-2009-0789 - OpenSSL Malformed ASN1 Structure Handling DoS
CVE-2009-1377 - OpenSSL ssl/d1_pkt.c dtls1_buffer_record Function Buffered DTLS Record Handling Remote DoS
CVE-2009-1378 - OpenSSL ssl/d1_both.c dtls1_process_out_of_seq_message Function DTLS Record Handling Remote Memory Consumption DoS
CVE-2009-1386 - OpenSSL ssl/s3_pkt.c DTLS ChangeCipherSpec Packet Handling Remote DoS
CVE-2009-1387 - OpenSSL ssl/d1_both.cdtls1_retrieve_buffered_fragment Function DTLS Handshake Message Fragment Remote DoS
CVE-2009-2409 - Network Security Services (NSS) Library X.509 Certificate MD2 Hash Collision Weakness

192.168.235.59 : Potential Vulnerabilities

Suggestions:

Upgrade to the latest version of OpenSSL. Please see http://www.openssl.org

PHP 5 < 5.2.7 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 35043
BID: 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32717, 32948, 33002, 33216
http://securityreason.com/achievement_securityalert/57
http://securityreason.com/achievement_securityalert/58
http://securityreason.com/achievement_securityalert/59
http://www.sektioneins.de/advisories/SE-2008-06.txt
http://archives.neohapsis.com/archives/fulldisclosure/2008-06/0238.html
http://archives.neohapsis.com/archives/fulldisclosure/2008-06/0239.html
http://www.openwall.com/lists/oss-security/2008/08/08/2 http://www.openwall.com/lists/oss-security/2008/08/13/8 http://archives.neohapsis.com/archives/fulldisclosure/2008-11/0433.html
http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0089.html
http://bugs.php.net/bug.php?id=42862
http://bugs.php.net/bug.php?id=45151
http://www.php.net/releases/5_2_7.php

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.7.

Such versions may be affected by several security issues :
- Missing initialization of 'BG(page_uid)' and 'BG(page_gid)' when PHP is used as an Apache module may allow for bypassing security restriction due to SAPI 'php_getuid()' overloading.
- Incorrect 'php_value' order for Apache configuration may allow bypassing PHP's 'safe_mode' setting.
- File truncation can occur when calling 'dba_replace()' with an invalid argument.
- The ZipArchive:extractTo() method in the ZipArchive extension fails to filter directory traversal sequences from file names.
- There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371)
- A buffer overflow in the 'imageloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)

192.168.235.59 : Potential Vulnerabilities

- There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659)
- When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg,'file..php'). (CVE-2008-3660)
- Multiple directory traversal vulnerabilities in functions such as 'posix_access()', 'chdir()', 'ftok()' may allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666).
- A buffer overflow may be triggered when processing long message headers in 'php_imap.c' due to use of an obsolete API call. (CVE-2008-2829)
- PHP 'proc_open()' Environment Parameter Safe Mode Restriction-Bypass Vulnerability
- PHP 'popen()' Function Buffer Overflow Vulnerability
- PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability (CVE-2008-5498)
- PHP 'mbstring' Extension Buffer Overflow Vulnerability (CVE-2008-5557)
- PHP SAPI 'php_getuid()' Safe Mode Restriction-Bypass Vulnerability (CVE-2008-5624)

Suggestions:

Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

PHP < 4.4.7 / 5.2.2 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2007-0455, CVE-2007-0911, CVE-2007-1001, CVE-2007-1285, CVE-2007-1375, CVE-2007-1396, CVE-2007-1399, CVE-2007-1460, CVE-2007-1461, CVE-2007-1484, CVE-2007-1521, CVE-2007-1522, CVE-2007-1581, CVE-2007-1582, CVE-2007-1583, CVE-2007-1649, CVE-2007-1709, CVE-2007-1710, CVE-2007-1717, CVE-2007-1718, CVE-2007-1864, CVE-2007-1883, CVE-2007-1886, CVE-2007-1888, CVE-2007-1900, CVE-2007-2509, CVE-2007-2510, CVE-2007-2727, CVE-2007-2748, CVE-2007-2872, CVE-2007-3007, CVE-2007-4670, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 25159
Bugtraq ID: 22764, 22289, 23357, 25159, 23818, 23813, 24034, 24012, 23984
CVE ID: 2007-1285, 2007-0455, 2007-1001, 2007-2509, 2007-2510, 2007-2748, 2007-2727

192.168.235.59 : Potential Vulnerabilities

FrSIRT Advisory: ADV-2007-0400, ADV-2007-1269, ADV-2007-2732
ISS X-Force ID: 33453
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-03/0319.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-04/0131.html
Mail List Post: http://attrition.org/pipermail/vim/2007-May/001621.html
News Article: http://www.techworld.com/security/news/index.cfm?newsID=8175
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070501-01-P.asc
Other Advisory URL: http://blog.php-security.org/archives/80-Watching-the-PHP-CVS.html
Other Advisory URL: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=224607
Other Advisory URL: http://docs.info.apple.com/article.html?artnum=306172
Other Advisory URL: http://en.securitylab.ru/nvd/292100.php
Other Advisory URL: http://fedoranews.org/cms/node/2631
Other Advisory URL: http://ifsec.blogspot.com/2007/04/php-521-wbmp-file-handling-integer.html
Other Advisory URL: http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00052.html
Other Advisory URL: http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00054.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00006.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00003.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-April/000176.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-February/000145.html
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-231.htm
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200705-19.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:035
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:036
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:038
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:089
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:187
Other Advisory URL: http://www.novell.com/linux/security/advisories/2007_15_sr.html
Other Advisory URL: http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=http--supportnovellcom-techcenter-psdb-3e349d7efffdfecc96ca44f446d1b2c4html&sliceId=&dialogID=38853114&stateId=0%200%2038851668
Other Advisory URL: http://www.php-security.org/MOPB/MOPB-03-2007.html
Other Advisory URL: http://www.php-security.org/MOPB/MOPB-14-2007.html
Other Advisory URL: http://www.slackware.org/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.470053
Other Advisory URL: http://www.trustix.org/errata/2007/0007/
Other Advisory URL: http://www.trustix.org/errata/2007/0017/
Other Advisory URL: http://www.ubuntu.com/usn/usn-462-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-473-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-549-1
Other Advisory URL: https://launchpad.net/bugs/cve/2007-1285
Other Solution URL: http://www.fortheloot.com/public/mcrypt.patch
RedHat RHSA: RHSA-2007:0163, RHSA-2007:0155, RHSA-2007:0154, RHSA-2007:0153, RHSA-2007:0889, RHSA-2007:0888
Secunia Advisory ID: 24941, 24924, 24910, 24909, 24945, 25445, 25816, 26048, 25192, 27864, 23916, 24053, 24052, 24022, 24107, 24143, 24151, 24965, 25575, 29157, 24814, 25151, 26235, 25255, 25318, 25365, 25372, 25660, 26967, 27351, 26895, 22588
Security Tracker: 1017771
Vendor Specific News/Changelog Entry: http://bugs.php.net/bug.php?id=40999

192.168.235.59 : Potential Vulnerabilities

Vendor Specific News/Changelog Entry: http://cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c?r1=1.2.4.1&r2=1.2.4.1.8.1
Vendor Specific News/Changelog Entry: http://cvs.php.net/viewvc.cgi/php-src/ext/gd/libgd/wbmp.c?revision=1.2.4.1.8.1&view=markup
Vendor Specific News/Changelog Entry: http://cvs.php.net/viewvc.cgi/php-src/ext/mcrypt/mcrypt.c?r1=1.91.2.3.2.9&r2=1.91.2.3.2.10
Vendor Specific News/Changelog Entry: http://us2.php.net/releases/4_4_7.php
Vendor Specific News/Changelog Entry: http://us2.php.net/releases/5_2_2.php
Vendor Specific News/Changelog Entry: http://viewcvs.php.net/viewvc.cgi/php-src/ext/soap/php_http.c?r1=1.77.2.11.2.5&r2=1.77.2.11.2.6
Vendor Specific News/Changelog Entry: http://www.php.net/ChangeLog-5.php
Vendor Specific News/Changelog Entry: http://www.php.net/ChangeLog-5.php#5.2.2
Vendor Specific News/Changelog Entry: http://www.php.net/releases/4_4_8.php
Vendor URL: http://www.php.net/
Vendor URL: http://www.zend.com/products/zend_engine

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 4.4.7 / 5.2.2.

Such versions may be affected by several issues, including buffer overflows in the GD library.

Suggestions:

Upgrade to PHP 4.4.7 / 5.2.2 or later. Please see: http://www.php.net

MySQL < 5.1

Impact: Level 5 - Urgent

CVE Reference: CVE-2004-0388, CVE-2004-0627, CVE-2004-0628, CVE-2005-1636, CVE-2005-2558, CVE-2005-2572, CVE-2005-2573, CVE-2006-0369, CVE-2006-0903, CVE-2006-1516, CVE-2006-1517, CVE-2006-1518, CVE-2006-2753, CVE-2006-3081, CVE-2006-3469, CVE-2006-3486, CVE-2006-4031, CVE-2006-4226, CVE-2006-4227, CVE-2006-7232, CVE-2007-1420, CVE-2007-2583, CVE-2007-2691, CVE-2007-2692, CVE-2007-5646, CVE-2007-6303, CVE-2007-6304, CVE-2008-2079, CVE-2008-4097, CVE-2008-4098, CVE-2008-4456, CVE-2009-2446

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 95135

Issue Description:

192.168.235.59 : Potential Vulnerabilities

MySQL version is older than 5.1.

According to the version number of the MySQL server banner on the remote host, the MySQL version may be vulnerable to a number of flaws, some of which allow code execution.
The vulnerabilities include the following (dependent on the version of MySQL DB running on the remote host):
CVE-2004-0388 - MySQL mysqld_multi Symlink Arbitrary File Overwrite
CVE-2004-0627 - MySQL Zero-length Scrambled String Crafted Packet Authentication Bypass
CVE-2004-0628 - MySQL Protocol 4.1 Authentication Scramble String Overflow
CVE-2005-1636 - MySQL mysql_install_db Symlink Arbitrary File Overwrite
CVE-2005-2558 - MySQL User-Defined Function init_syms() Function Overflow
CVE-2005-2572 - MySQL UDF LoadLibraryEx Function Nonexistent Library Load DoS
CVE-2005-2573 - MySQL on Windows UDF Create Function Traversal Privilege Escalation
CVE-2006-0369 - MySQL VIEW Access information_schema.views Information Disclosure
CVE-2006-0903 - MySQL Query NULL Charcter Logging Bypass
CVE-2006-1516 - MySQL Malformed Login Packet Remote Memory Disclosure
CVE-2006-1517 - MySQL Crafted COM_TABLE_DUMP Request Arbitrary Memory Disclosure
CVE-2006-1518 - MySQL COM_TABLE_DUMP Packet Overflow
CVE-2006-2753 - MySQL Multibyte Encoding SQL Injection Filter Bypass
CVE-2006-3081 - MySQL mysqld str_to_date Function NULL Argument DoS
CVE-2006-3469 - MySQL Server time.cc date_format Function Format String
CVE-2006-3486 - MySQL Instance_options::complete_initialization Function Overflow
CVE-2006-4031 - MySQL MERGE Table Privilege Persistance
CVE-2006-4226 - MySQL Case Sensitivity Unauthorized Database Creation
CVE-2006-4227 - MySQL SUID Routine Miscalculation Arbitrary DML Statement Execution
CVE-2006-7232 - MySQL sql_select.cc INFORMATION_SCHEMA Table Crafted Query Remote DoS
CVE-2007-1420 - MySQL information_schema Table Subselect Single-Row DoS
CVE-2007-2583 - MySQL Crafted IF Clause Divide-by-zero NULL Dereference DoS
CVE-2007-2691 - MySQL RENAME TABLE Statement Arbitrary Table Name Modification
CVE-2007-2692 - MySQL mysql_change_db Function THD::db_access Privilege Escalation
CVE-2007-5646 - Simple Machines Forum (SMF) Sources/Search.php SQL Injection
CVE-2007-6303 - MySQL DEFINER View Value Crafted Statements Remote Privilege Escalation
CVE-2007-6304 - MySQL Federated Engine SHOW TABLE STATUS Query Remote DoS
CVE-2008-2079 - MySQL MyISAM Table CREATE TABLE Privilege Check Bypass
CVE-2008-4097 - MySQL MyISAM Table CREATE TABLE Privilege Check Bypass
CVE-2008-4098 - MySQL MyISAM Table CREATE TABLE Privilege Check Bypass
CVE-2008-4456 - MySQL Command Line Client HTML Output XSS
CVE-2009-2446 - MySQL sql_parse.cc dispatch_command() Function Format String DoS

Suggestions:

Upgrade to the latest version of MySQL. Please see: http://dev.mysql.org

PHP < 5.2.3 Multiple Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 10

192.168.235.59 : Potential Vulnerabilities

CVE Reference: CVE-2006-1549, CVE-2007-1396, CVE-2007-1460, CVE-2007-1521, CVE-2007-1581, CVE-2007-1582, CVE-2007-1583, CVE-2007-1717, CVE-2007-1718, CVE-2007-1835, CVE-2007-1900, CVE-2007-2510, CVE-2007-2727, CVE-2007-2748, CVE-2007-2756, CVE-2007-2844, CVE-2007-2872, CVE-2007-3007, CVE-2008-0599, CVE-2008-2050, CVE-2008-2051, CVE-2008-2107, CVE-2008-2108, CVE-2008-2666, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-4107, CVE-2008-5498, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-5814, CVE-2009-1271, CVE-2009-1272

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 25368
Bugtraq ID: 22766, 22886, 22954, 22968, 23016, 23046, 23062, 23119, 23145, 23146, 23183, 23202, 23359, 23984, 24012, 24034, 24089, 24109, 24259, 24261, 24268, 24661, 25498, 26426, 32688, 32717, 32948, 33002, 33216, 33542
CVE ID: 2007-1900, 2007-2756, 2007-3007, 2007-2872
FrSIRT Advisory: ADV-2007-1905, ADV-2007-1904, ADV-2007-2016, ADV-2007-2336, ADV-2007-3386, ADV-2007-2061
ISS X-Force ID: 33510
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0005.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0102.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0079.html
Other Advisory URL: HPSBUX02262 SSRT071447
Other Advisory URL: HPSBUX02308 SSRT080010
Other Advisory URL: HPSBUX02332 SSRT080056
Other Advisory URL: http://blog.php-security.org/archives/86-Chunk_split-Overflow-not-fixed-at-all....html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-07/msg00006.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00006.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-June/000196.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-October/000269.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-September/000244.html
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.399824
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.482863
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-449.htm
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200705-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200710-02.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-34.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200805-13.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:122
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:123
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:124
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:187
Other Advisory URL: http://www.novell.com/linux/security/advisories/2007_13_sr.html

192.168.235.59 : Potential Vulnerabilities

Other Advisory URL: http://www.openpkg.com/security/advisories/OpenPKG-SA-2007.020.html
Other Advisory URL: http://www.php-security.org/MOPB/PMOPB-45-2007.html
Other Advisory URL: http://www.php.net/releases/5_2_3.php
Other Advisory URL: http://www.sec-consult.com/291.html
Other Advisory URL: http://www.trustix.org/errata/2007/0019/
Other Advisory URL: http://www.trustix.org/errata/2007/0023/
Other Advisory URL: http://www.ubuntu.com/usn/usn-455-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-473-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-549-1
Other Advisory URL: http://www.us.debian.org/security/2007/dsa-1283
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00321.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00354.html
RedHat RHSA: RHSA-2007:0890, RHSA-2007:0889, RHSA-2007:0888
Related OSVDB ID: 36083, 36084
Secunia Advisory ID:24824, 25057, 25062, 25353, 25362, 25378, 25445, 25456, 25535, 25575, 25590, 25646, 25657, 25658, 25787, 26048, 26231, 26390, 26748, 26802, 26838, 26871, 26895, 26930, 26967, 27037, 27102, 27351, 27377, 27545, 27759, 27864, 28658, 28750, 29157, 30040, 30168
Security Tracker: 1018186, 1018187
Vendor Specific News/Changelog Entry: http://bugs.libgd.org/?do=details&task_id=86
Vendor Specific News/Changelog Entry: http://bugs.php.net/bug.php?id=41492
Vendor Specific News/Changelog Entry: http://www.libgd.org/ReleaseNote020035
Vendor Specific News/Changelog Entry: http://www.php.net/releases/5_2_3.php
Vendor URL: http://www.php.net/

Issue Description:

According to its banner, the version of PHP installed on the remote host is older than 5.2.3.

Such versions may be affected by several issues, including an integer overflow, 'safe_mode' and 'open_basedir' bypass, and a denial of service vulnerability.

Suggestions:

Upgrade to PHP version 5.2.3 or later. Please see: http://www.php.net

PHP cURL "safe_mode" and "open_basedir" Restriction Bypass Vulnerability

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95176

192.168.235.59 : Potential Vulnerabilities

Bugtraq ID: 34475

Issue Description:

PHP is a scripting language that is suited for Web development and can be embedded into HTML.
PHP is prone to a security vulnerability that allows an attacker to bypass restrictions because of improper checking of arguments to cURL functions "safe_mode" and "open_basedir". An attacker can exploit this flaw by prefixing a file location with "file:/" in combination with a specially crafted virtual tree to bypass access restrictions to view files without authorization.
This vulnerability would be an issue in shared-hosting configurations where multiple users can create and execute arbitrary PHP script code, with the "safe_mode" and "open_basedir" restrictions are used to isolate the users from each other.
PHP 5.2.9 is vulnerable; other versions may also be affected.

Successful exploitation of this vulnerability could allow disclosure of sensitive information by exposing files that are not normally accessible.

Suggestions:

Avoid the use of "safe_mode" and "open_basedir" as main security functions.
Patch:
There are no vendor-supplied patches available at this time. For the latest updates visit the PHP Web site.

PHP "dba_replace()" File Corruption Vulnerability

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95178
Bugtraq ID: 33498

Issue Description:

PHP is a general-purpose scripting language that is especially suited for web development and can be embedded into HTML. The "dba_replace" function allows replacing or insertion of entries.
PHP is prone to a database file corruption vulnerability that is caused due to improper input validation.
The problem occurs when performing actions on a Berkely DB style database with the "dba_replace()" function. Specifically, the function does not filter strings keys and/or values failing to properly validate the "key" before performing actions on the database. An attacker that can control the "key" value can cause the database to be truncated or cause arbitrary destruction of files.
PHP Version 5.2.6 is vulnerable; prior versions may also be affected.

192.168.235.59 : Potential Vulnerabilities

If this vulnerability is successfully exploited, attackers can cause corruption of the database files resulting in loss of data. Successful attempts may also lead to denial of service for legitimate users.

Suggestions:

Upgrade to the latest version of PHP.

MySQL Community Server 5.0 < 5.0.67 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2006-4226, CVE-2006-4227, CVE-2006-7232, CVE-2007-2583, CVE-2007-2691, CVE-2007-2692, CVE-2007-5969, CVE-2007-6303, CVE-2007-6304, CVE-2008-0226, CVE-2008-0227, CVE-2008-2079, CVE-2008-4456

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 34159
BID: 19559, 24011, 24016, 26765, 26832, 27140, 28351, 29106, 31486
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-67.html http://lists.mysql.com/announce/542

Issue Description:

The version of MySQL Enterprise Server 5.0 installed on the remote host is before 5.0.66.

Such versions are reportedly affected by the following issues :
- When using a FEDERATED table, a local server could be forced to crash if the remote server returns a result with fewer columns than expected (Bug #29801).
- ALTER VIEW retains the original DEFINER value, even when altered by another user, which could allow that user to gain the access rights of the view (Bug #29908).
- A local user can circumvent privileges through creation of MyISAM tables using the 'DATA DIRECTORY' and 'INDEX DIRECTORY' options to overwrite existing table files in the application's data directory (Bug #32167).
- RENAME TABLE against a table with DATA/INDEX DIRECTORY overwrites the file to which the symlink points (Bug #32111). - It was possible to force an error message of excessive length, which could lead to a buffer overflow (Bug #32707).
- Three vulnerabilities in yaSSL versions 1.7.5 and earlier as used in MySQL could allow an unauthenticated remote attacker to crash the server or to execute arbitrary code provided yaSSL is enabled and the server allows TCP connections (Bug #33814).

Suggestions:

192.168.235.59 : Potential Vulnerabilities

Upgrade to MySQL Community Server version 5.0.67.

Apache < 2.2.8 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423, CVE-2007-6514, CVE-2008-0005, CVE-2008-0455, CVE-2008-0456, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 31118
Bugtraq ID: 26663, 26838, 27234, 27236, 27237, 27409, 8707
CVE ID: 2007-6203, 2007-5000, 2007-6388, 2008-0005, 2007-6420,2007-6421, 2007-6422, 2007-6423
FrSIRT Advisory: ADV-2007-4060, ADV-2007-4201, ADV-2007-4202, ADV-2007-4301, ADV-2008-0047, ADV-2008-0048
ISS X-Force ID: 38800, 39002, 39001, 39615
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0135.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0193.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-03/0159.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-11/0150.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Other Advisory URL: HPSBUX02308 SSRT080010
Other Advisory URL: HPSBUX02313 SSRT080015
Other Advisory URL: HPSBUX02431 SSRT090085
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2008-July/000370.html
Other Advisory URL: http://procheckup.com/Vulnerability_PR07-37.php
Other Advisory URL: http://securityreason.com/achievement_securityalert/49
Other Advisory URL: http://securityreason.com/securityalert/3523
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-233623-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK62966
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200801e.html

192.168.235.59 : Potential Vulnerabilities

Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200807e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200808e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200803-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:014
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:015
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
Other Advisory URL: https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/install/v61.Readme.html#MH01110
RedHat RHSA: RHSA-2008:0004, RHSA-2008:0005, RHSA-2008:0006, RHSA-2008:0007, RHSA-2008:0008
Secunia Advisory ID: 27906, 28046, 28073, 28081, 28082, 28196, 28375, 28467, 28471, 28525, 28526, 28607, 28749, 28750, 28922, 28965, 28977, 29348, 29420, 29504, 29640, 29806, 29988, 30356, 30430, 30732, 31026, 31142, 32222, 32575, 32800, 33105, 33200, 33797, 34219, 34219, 35650
Security Tracker: 1019030, 1019093, 1019154, 1019185
Snort Signature ID: 13302
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1897
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-042_e/index-e.html
Vendor Specific Advisory URL: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01756421
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_20.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58074
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg24019245
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: ftp://ftp.software.ibm.com/software/websphere/ihs/support/fixes/PK65782/

Issue Description:

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8.

Such versions may be affected by several issues, including:
- A cross-site scripting issue involving mod_imagemap (CVE-2007-5000).
- A cross-site scripting issue involving 413 error pages via a malformed HTTP method (PR 44014 / CVE-2007-6203).
- A cross-site scripting issue in mod_status involving the refresh parameter (CVE-2007-6388).
- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

192.168.235.59 : Potential Vulnerabilities

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi-Processing Module is used (CVE-2007-6422).
- A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset (CVE-2008-0005).
- Apache 'mod_negotiation' HTML Injection and HTTP Response Splitting Vulnerability (CVE-2008-0455, CVE-2008-0456)
Note: that the remote web server may not actually be affected by these vulnerabilities. HackRack did not try to determine whether the affected modules are in use or to check for the issues themselves.

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

Apache < 2.2.6 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2006-4110, CVE-2006-4154, CVE-2006-5752, CVE-2007-1741, CVE-2007-1742, CVE-2007-1743, CVE-2007-1862, CVE-2007-1863, CVE-2007-3303, CVE-2007-3304, CVE-2007-3847, CVE-2007-4465, CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423, CVE-2008-0455, CVE-2008-2168, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2008-1678

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 26023
Bugtraq ID: 24215, 24553, 24645, 24649, 25489, 25653, 21865, 25653
CVE ID: 2007-3303, 2007-3847, 2006-5752, 2007-4465, 2007-1862, 2007-3304
FrSIRT Advisory: ADV-2007-2727, ADV-2007-3100, ADV-2007-3020, ADV-2007-3095, ADV-2007-3283, ADV-2007-3494, ADV-2007-2231
ISS X-Force ID: 36586
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0415.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0251.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0129.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0102.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0184.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://mail-archives.apache.org/mod_mbox/httpd-dev/200706.mbox/%3c20070629141032.GA15192@redhat.com%3e
Mail List Post: http://marc.info/?l=apache-cvs&m=118592992309395&w=2
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118252946632447&w=2

192.168.235.59 : Potential Vulnerabilities

Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118595556504202&w=2

Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118595953217856&w=2
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc
Other Advisory URL: HPSBUX02262 SSRT071447
Other Advisory URL: HPSBUX02273 SSRT071476
Other Advisory URL: HPSBUX02365 SSRT080118
Other Advisory URL: HPSBUX02431 SSRT090085
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:140
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:141
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:142
Other Advisory URL: http://httpd.apache.org/security/vulnerabilities_20.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-11/msg00002.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-June/000207.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-September/000241.html
Other Advisory URL: http://security.psnc.pl/files/apache_report.pdf
Other Advisory URL: http://securityreason.com/achievement_securityalert/46
Other Advisory URL: http://securityreason.com/securityalert/2814
Other Advisory URL: http://securityreason.com/securityalert/3113
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-103179-1
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-200032-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-351.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-363.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-500.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK49295
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK50467
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK50469
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702
Other Advisory URL: http://www-1.ibm.com/support/search.wss?rs=0&q=PK50467&apar=only
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200807e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:235
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:140
Other Advisory URL: http://www.redhat.com/errata/RHSA-2007-0532.html
Other Advisory URL: http://www.redhat.com/support/errata/RHSA-2007-0557.html
Other Advisory URL: http://www.redhat.com/support/errata/RHSA-2007-0662.html
Other Advisory URL: http://www.trustix.org/errata/2007/0026/
Other Advisory URL: http://www.ubuntu.com/usn/usn-499-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00353.html
RedHat RHSA: RHSA-2007:0532, RHSA-2007:0556, RHSA-2007:0557, RHSA-2007:0662, RHSA-2007:0746, RHSA-2007:0534, RHSA-2007:0533, RHSA-2007:0911
Related OSVDB ID: 38939, 37050

192.168.235.59 : Potential Vulnerabilities

Secunia Advisory ID: 26273, 25920, 25827, 25830, 26211, 26443, 26508, 26611, 26759, 26790, 26822, 27209, 27563, 27732, 26636, 26722, 26952, 26842, 27593, 27882, 27971, 28467, 28606, 28749, 28922, 26993, 29420, 30430, 25873, 27037, 26458, 28224, 28471, 28082, 28607, 31651, 33105, 35650
Security Tracker: 1018304, 1018633, 1018302
Snort Signature ID: 13309, 13310, 13311
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1897
Vendor Specific Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-041_e/index-e.html
Vendor Specific Advisory URL: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01756421
Vendor Specific News/Changelog Entry: http://bugs.gentoo.org/show_bug.cgi?id=186219
Vendor Specific News/Changelog Entry: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=245111
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_20.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://issues.apache.org/bugzilla/show_bug.cgi?id=41551
Vendor Specific News/Changelog Entry: http://issues.apache.org/bugzilla/show_bug.cgi?id=41551>
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=547987
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=549159
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006876
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/CHANGES_2.2.6
Vendor Specific News/Changelog Entry: http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1500
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc

Issue Description:

According to its banner, the version of Apache installed on the remote host is older than 2.2.6. Such versions may be affected by several issues.

These issues include :
- A denial of service vulnerability in mod_proxy.
- A cross-site scripting vulnerability in mod_status.
- A local denial of service vulnerability associated with the Prefork MPM module.
- An information leak in mod_cache.
- A denial of service vulnerability in mod_cache.

In addition, it offers a workaround for a cross-site scripting issue in mod_autoindex.
Note: the remote web server may not actually be affected by these vulnerabilities. The scanner did not try to determine whether any of the affected modules are in use on the remote server or to check for the issues themselves.

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.6 or later.

MySQL Community Server 5.0 < 5.0.51 RENAME TABLE Symlink System Table Overwrite

192.168.235.59 : Potential Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 4

CVE Reference: CVE-2007-5925, CVE-2007-5969

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 29251
BID: 26765
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-51.html
http://forums.mysql.com/read.php?3,186931,186931

Issue Description:

The remote database server is susceptible to a local symlink attack.

The version of MySQL Community Server installed on the remote host reportedly fails to check whether a file to which a symlink points exists when using RENAME TABLE against a table with explicit DATA DIRECTORY and INDEX DIRECTORY options. A local attacker may be able to leverage this issue to overwrite system table information by replacing the file to which the symlink points.

Suggestions:

Upgrade to MySQL Community Server version 5.0.51 or later.

Apache 2.2 < 2.2.14 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2009-2699, CVE-2009-3094, CVE-2009-3095

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 42052
http://www.securityfocus.com/advisories/17947
http://www.securityfocus.com/advisories/17959
http://www.intevydis.com/blog/?p=59
https://issues.apache.org/bugzilla/show_bug.cgi?id=47645
http://www.apache.org/dist/httpd/CHANGES_2.2.14

192.168.235.59 : Potential Vulnerabilities

BID:36254
OSVDB:57851, OSVDB:58879, Secunia:36549

Issue Description:

The remote web server is affected by multiple vulnerabilities.

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14.
Such versions are potentially affected by multiple vulnerabilities :
- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)
- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions.
(CVE-2009-3095)
- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp'module allows
remote FTP servers to cause a denial-of-service. (CVE-2009-3094)
Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not
try to determine whether the affected modules are in use or check for the issues themselves.

Suggestions:

Either ensure the affected modules are not in use or upgrade to Apache
version 2.2.14 or later.

Apache < 2.2.9 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2007-6420, CVE-2007-6423, CVE-2008-0455, CVE-2008-0456, CVE-2008-2364, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2007-6421, CVE-2007-6422

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 33477
Bugtraq ID: 27236, 29653, 8707, 27409
CVE ID: 2007-6420, 2007-6421, 2007-6422, 2007-6423, 2008-2364
FrSIRT Advisory: ADV-2008-0048, ADV-2008-1798
ISS X-Force ID: 42987
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Other Advisory URL: HPSBUX02365 SSRT080118
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html

192.168.235.59 : Potential Vulnerabilities

Other Advisory URL: http://securityreason.com/securityalert/3523
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg27008517
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200803-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
RedHat RHSA: RHSA-2008:0008
Secunia Advisory ID: 28526, 28749, 28977, 29348, 29420, 29640, 30621, 31026, 31404, 31416, 31651, 31904, 32222, 32575, 32685, 32838, 33156, 33797, 34219, 34259, 34418
Security Tracker: 1020267
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html

Issue Description:

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9.
There are a number of vulnerabilities that affect version prior to 2.2.9.

Such versions may be affected by several issues, including:;;
- Improper handling of excessive forwarded interim responses may cause denial-of-service conditions in mod_proxy_http (CVE-2008-2364).
- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer (CVE-2007-6420).;
- Apache htpasswd Password Entropy Weakness;
- Apache 'mod_negotiation' HTML Injection and HTTP Response Splitting Vulnerability;
Note: that the remote web server may not actually be affected by these vulnerabilities.
HackRack/BroadView did not try to determine whether the affected modules are in use or to check for the issues themselves.

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

192.168.235.59 : Potential Vulnerabilities

MySQL Community Server 5.0 < 5.0.51 RENAME TABLE Symlink Syster Table Overwrite

Impact: Level 4 - Critical

CVSS Score: 4

CVE Reference: CVE-2007-5925, CVE-2007-5969

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 29251
BID: 26765
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-51.html
http://forums.mysql.com/read.php?3,186931,186931

Issue Description:

The remote database server is susceptible to a local symlink attack.

The version of MySQL Community Server installed on the remote host reportedly fails to check whether a file to which a symlink points exists when using RENAME TABLE against a table with explicit DATA DIRECTORY and INDEX DIRECTORY options. A local attacker may be able to leverage this issue to overwrite system table information by replacing the file to which the symlink points.

Suggestions:

Upgrade to MySQL Community Server version 5.0.51 or later.

MySQL Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Fur Denial of Service Vulnerability

Impact: Level 4 - Critical

CVSS Score: 4

CVE Reference: CVE-2007-5925

Port/Protocol: 3306/TCP

Other References:

192.168.235.59 : Potential Vulnerabilities

Nessus NASL ID : 95177
Bugtraq ID: 26353

Issue Description:

MySQL is a freely available SQL database for multiple platforms.
MySQL is prone to a remote denial of service vulnerability because it fails to properly handle unexpected conditions. The database server crashes when trying to process an SQL query using the 'CONTAINS' argument along with the 'FULLTEXT' index in the InnoDB engine.
This issue affects MySQL Versions 5.1.23 and prior.

This issue allows remote attackers to crash affected database servers, denying service to legitimate users.

Suggestions:

There are no vendor-supplied patches available at this time.

PHP 'popen()' Function Buffer Overflow Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95235
BugTraq ID: 33216

Issue Description:

PHP is a general purpose scripting language that is especially suited for web development and can be embedded into HTML. The "popen" function opens a pipe to the program specified in the command parameter.
PHP is prone to a buffer overflow vulnerability that occurs in the "popen" function because it fails to perform adequate boundary checks before copying user-supplied data to insufficiently sized memory buffers. This issue can be exploited by passing a large string to the "mode" argument of the function.
PHP 5.2.8 and prior versions are affected.

If this vulnerability is successfully exploited, a malicious user can execute arbitrary machine code in the context of the affected Web server. Failed attempts cause denial of service attacks by crashing the Web server.

Suggestions:

There are no vendor-supplied patches available at this time. For the latest information, visit the PHP

192.168.235.59 : Potential Vulnerabilities

Web site.

MySQL Crafted IF Clause Divide-by-zero NULL Dereference DoS

Impact: Level 3 - High

CVSS Score: 4

CVE Reference: CVE-2007-2583

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 25198
BID: 23911
http://bugs.mysql.com/bug.php?id=27513
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-41.html
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-40.html

Issue Description:

The remote database server is prone to a denial of service attack.

The version of MySQL installed on the remote host reportedly is affected by a denial of service vulnerability that may be triggered with a specially crafted IF query. An attacker who can execute arbitrary SELECT statements may be able to leverage this issue to crash the affected service.

Suggestions:

Upgrade to MySQL Community Server 5.0.41 / 5.1.18 / Enterprise Server 5.0.40 or later.

MySQL Single Row Subselect Remote DoS

Impact: Level 3 - High

CVSS Score: 3.5

CVE Reference: CVE-2007-1420, CVE-2006-7232

Port/Protocol: 3306/TCP

Other References:

192.168.235.59 : Potential Vulnerabilities

Nessus NASL ID : 24905
BID: 22900
http://www.sec-consult.com/284.html
http://www.securityfocus.com/archive/1/archive/1/462339/100/0/threaded
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-37.html

Issue Description:

According to its banner, the version of MySQL on the remote host is older than 5.0.37.

Such versions are vulnerable to a remote denial of service when processing certain single row subselect queries. A malicious user can crash the service via a specially-crafted SQL query.

Suggestions:

Upgrade to MySQL version 5.0.37 or newer.

Apache 2.x < 2.2.12 Multiple Vulnerabilities

Impact: Level 3 - High

CVE Reference: CVE-2008-2939, CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 40467
Bugtraq ID: 30560, 34663, 35221, 35253
CERT VU: 663763
CVE ID: 2008-2939, 2009-1191, 2009-1195, 2009-0023, 2009-1955, 2009-1956, 2009-1890, 2009-1891

Issue Description:

The remote web server may be affected by several issues.

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12.
Such versions may be affected by several issues, including :
- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)
- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)
- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to

192.168.235.59 : Potential Vulnerabilities

bypass security restrictions. (CVE-2009-1195)
- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy
configuration. (CVE-2009-1890)
- Failure of mod_deflate to stop compressing a file when
the associated network connection is closed may allow a
remote attacker to consume large amounts of CPU if
there is a large (>10 MB) file available that has
mod_deflate enabled. (CVE-2009-1891)
- Using a specially crafted XML document with a large
number of nested entities, a remote attacker may be
able to consume an excessive amount of memory due to
a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)
- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-
util library in the way it handles a variable list of arguments, which could be leveraged on big-endian
platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)
Note that Nessus has relied solely on the version in the Server response header and did not try to check
for the issues themselves or even whether the affected modules are in use.

Suggestions:

Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12
or later.

MySQL Enterprise Server 5.0 < 5.0.66 Empty Bit-String Literal Token SQL Statement DoS

Impact: Level 3 - High

CVSS Score: 4

CVE Reference: CVE-2008-3963

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 34162
http://bugs.mysql.com/bug.php?id=35658
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-66.html
http://www.openwall.com/lists/oss-security/2008/09/09/4
http://www.openwall.com/lists/oss-security/2008/09/09/7
BID:31081
OSVDB:48021

Issue Description:

192.168.235.59 : Potential Vulnerabilities

The remote database server is susceptible to a denial of service attack.

Suggestions:

No suggestion at this time

MySQL 5.1 < 5.1.32 XPath Expression DoS

Impact: Level 3 - High

CVSS Score: 4

CVE Reference: CVE-2009-0819

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 35766

Suggestions:

No suggestion at this time

MySQL Community Server 5.0 < 5.0.45 Multiple Vulnerabilities

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2007-3780, CVE-2007-3781, CVE-2007-3782

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 25759
BID: 25017
http://dev.mysql.com/doc/refman/5.0/en/releasenotes-cs-5-0-45.html

Issue Description:

The remote database server is susceptible to multiple attacks.

192.168.235.59 : Potential Vulnerabilities

The version of MySQL Community Server installed on the remote host reportedly is affected by a denial of service vulnerability that can lead to a server crash with a specially-crafted password packet.
It is also affected by a privilege escalation vulnerability because 'CREATE TABLE LIKE' does not require any privileges on the source table, which allows an attacker to create arbitrary tables using the affected application.

Suggestions:

Upgrade to MySQL Community Server version 5.0.45 or later.

PHP < 5.2.10 Multiple Vulnerabilities

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2009-2687

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 39480
http://bugs.php.net/bug.php?id=45997
http://bugs.php.net/bug.php?id=48378
http://www.php.net/releases/5_2_10.php
http://www.php.net/ChangeLog-5.php#5.2.10

Issue Description:

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :
- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)
- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

Suggestions:

Upgrade to PHP version 5.2.10 or later. Please see: http://www.php.net

MySQL 5.1 < 5.1.18 Multiple Vulnerabilities

192.168.235.59 : Potential Vulnerabilities

Impact: Level 3 - High

CVSS Score: 6

CVE Reference: CVE-2007-2583, CVE-2007-2691, CVE-2007-2692, CVE-2007-2693

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 25242
http://bugs.mysql.com/bug.php?id=23675
http://bugs.mysql.com/bug.php?id=27515
http://bugs.mysql.com/bug.php?id=27337
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html
BID:23911
OSVDB:34734, OSVDB:34765, OSVDB:34766, OSVDB:37781

Issue Description:

The remote database server is affected by multiple vulnerabilities.

Suggestions:

No suggestion at this time

Apache 2.2 < 2.2.11

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2008-2939, CVE-2008-2364, CVE-2009-1191

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95123
Bugtraq ID: 29653, 30560, 34663
CERT VU: 663763
CVE ID: 2008-2364, 2008-2939, 2009-1191
FrSIRT Advisory: ADV-2008-1798, ADV-2008-2315, ADV-2008-2461
ISS X-Force ID: 42987, 44223, 50059
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0051.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html

192.168.235.59 : Potential Vulnerabilities

Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Mail List Post: http://marc.info/?l=bugtraq&m=123376588623823&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/495180/100/0/threaded
Other Advisory URL: HPSBUX02365 SSRT080118:
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg27008517
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200809e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
Other Advisory URL: http://www.rapid7.com/advisories/R7-0033
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html
RedHat RHSA: RHSA-2008:0966, RHSA-2008:0967
Related OSVDB ID: 47474
Secunia Advisory ID: 30621, 31026, 31384, 31404, 31416, 31651, 31673, 31904, 32222, 32575, 32685, 32838, 33156, 33428, 33797, 33933, 34219, 34259, 34418, 34827, 35074, 35395, 35721
Security Tracker: 1020267
Security Tracker: 1020635
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1222
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200907-04.xml
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682868
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682870
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682871
Vendor Specific News/Changelog Entry: https://issues.apache.org/bugzilla/show_bug.cgi?id=46949
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-June/000915.html
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
Vendor Specific Solution URL: http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

192.168.235.59 : Potential Vulnerabilities

Issue Description:

Apache 2.2 version is older than 2.2.11.

According to the version number of the Apache banner on the remote host, the Apache 2.2 version may be vulnerable to a number of flaws, some of which allow code execution.
These include the following:
CVE-2008-2939 - Apache mod_proxy_ftp Directory Component Wildcard Character XSS
CVE-2008-2364 - Apache mod_proxy ap_proxy_http_process_response() Function Interim Response Forwarding Remote DoS
CVE-2009-1191 - Apache mod_proxy_ajp Cross Thread/Session Information Disclosure

Suggestions:

Upgrade to the latest version of Apache 2.2. Please see: http://httpd.apache.org

PHP < 5.2.11 Multiple Vulnerabilities

Impact: Level 3 - High

CVE Reference: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 41014
http://www.php.net/releases/5_2_11.php
http://news.php.net/php.internals/45597
http://www.php.net/ChangeLog-5.php#5.2.11
BID:36449
Secunia:36791

Issue Description:

The remote web server uses a version of PHP that is affected by
multiple flaws.

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :
- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.
- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.
- An unspecified input validation vulnerability affects exif processing.
- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

Suggestions:

192.168.235.59 : Potential Vulnerabilities

Upgrade to PHP version 5.2.11 or later.

MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability

Impact: Level 3 - High

CVSS Score: 2.6

CVE Reference: CVE-2008-4456

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 95231
BugTraq ID: 31486
http://bugs.mysql.com/bug.php?id=27884

Issue Description:

MySQL is prone to an HTML injection vulnerability because the application's command-line client fails to properly sanitize user-supplied input before using it in dynamically generated content.

Attacker-supplied HTML and script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

Suggestions:

MYSQL has released a patch to address this issue. Refer to MySQL Bug #27884 for further details on these vulnerabilities and patch instructions.

PHP 'mbstring.func_overload' Webserver Denial of Service Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

192.168.235.59 : Potential Vulnerabilities

Nessus NASL ID : 95234
BugTraq ID: 33542

Issue Description:

The "mbstring.func_overload" PHP directive in php.ini is used to overload a set of single byte functions.
A denial of service vulnerability exists in PHP because the globalscope for "mbstring_func.overload" directive related to unicode text operations is not set appropriately when it is used in a virtual server.
When "mbstring.func_overload" is set to 7 in a .htaccess file, it causes the setting to be set globally for the Web server breaking most unicode text operations and hampering other sites hosted by the Web server.
PHP Versions 5.2.5 and earlier are affected.

If this vulnerability is successfully exploited, it will allow malicious users to crash the affected Web server causing a denial of service.

Suggestions:

Upgrade to the latest version of PHP.

PHP 5.3 < 5.3.1 Multiple Vulnerabilities

Impact: Level 3 - High

CVSS Score: 7.5

CVE Reference: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2009-3558

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 42862
http://www.securityfocus.com/archive/1/507982/30/0/threaded
http://www.php.net/releases/5_3_1.php
http://www.php.net/ChangeLog-5.php#5.3.1
BID:36554
Secunia:37412

Issue Description:

The remote web server uses a version of PHP that is affected by multiple flaws.

Suggestions:

192.168.235.59 : Potential Vulnerabilities

No suggestion at this time

MySQL Create Database Bypass and Privilege Escalation (RHSA-2007-0152, RHSA-2007-0083)

Impact: Level 2 - Medium

CVSS Score: 6.5

CVE Reference: CVE-2006-4226, CVE-2006-4227

Port/Protocol: 3306/TCP

Other References:

Nessus NASL ID : 95232
http://rhn.redhat.com/errata/RHSA-2007-0152.html
http://rhn.redhat.com/errata/RHSA-2007-0083.html

Issue Description:

MySQL is exposed to vulnerabilities which can be exploited by malicious users to bypass certain security restrictions.
1) A user, who has been granted access to a certain database but not privileges to create additional databases, can create a database where the name differs only by the case of one or more letters from the database which the user has access to. Successful exploitation requires that MySQL runs on a system with a file system supporting case-sensitive file names.
2) An error caused due to arguments to "suid" routines being calculated in an incorrect security context can be exploited to execute arbitrary DML statements with the privileges of the routine's definer via a stored routine.
Successful exploitation requires that the user has "EXECUTE" privileges on the stored routine.

Malicious users can exploit these vulnerabilities to bypass certain security restrictions and perform certain actions with escalated privileges.

Suggestions:

Update to MySQL Version 5.0.25 or later.
Red Hat has released following advisories to address the issue:
RHSA-2007:0152
RHSA-2007:0083

Apache Web Server ETag Header Information Disclosure Weakness

Impact: Level 2 - Medium

192.168.235.59 : Potential Vulnerabilities

CVSS Score: 4.3

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95175
Bugtraq ID: 6939

Issue Description:

The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.
A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.
A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client. In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in in ETag headers. In later versions, the default behavior is to release this sensitive information.

This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

Suggestions:

OpenBSD has released a patch that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.
Customers are advised to upgrade to the latest version of Apache. In Apache Version 1.3.23 and later, it's possible to configure the FileETag directive to generate ETag headers without inode information.
To do so, include 'FileETag -INode' in the Apache server configuration file for a specific subdirectory.
In order to fix this vulnerability globally, for the Web server, use the option 'FileETag None'. Use the option 'FileETag
MTime Size' if you just want to remove the Inode information.

192.168.235.60 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
Solaris 10

Open Ports

Port	Protocol	Service	Comment
21	tcp	ftp	Banner - 220 sunnyjim FTP server ready.
22	tcp	ssh	Banner - SSH-2.0-Sun_SSH_1.1
23	tcp	telnet	Banner - login:
25	tcp	smtp	Banner - 220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Mon, 7 Dec 2009 09:20:26 -0500 (EST)
79	tcp	finger	Service - Finger
111	tcp	sunrpc	Service - RPC Portmapper
111	udp	sunrpc	Service - RPC Portmapper
161	udp	snmp	Service - SNMP
177	udp	xdmcp	Sevrice - xdmcp
513	tcp	login	Service - login
514	tcp	shell	tcpwrapped
514	udp	syslog	Service - syslog
587	tcp	submission	Banner - 220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7; Mon, 7 Dec 2009 09:21:20 -0500 (EST)
4045	tcp	lockd	Service - rpcbind
6000	tcp	x11	Service - X11
6112	tcp	dtspcd	Service - dtspc
6788	tcp	smc-http	Banner - Server: Apache-Coyote/1.1
6789	tcp	smc-https	Banner - Server: Apache-Coyote/1.1
7100	tcp	font-service	Service - font-service
32771	tcp	filenet-rmi	Service - rpcbind
32771	udp	filenet-rmi	Service - sometimes-rpc6
32772	tcp	filenet-pa	Service - rpcbind
32775	tcp	sometimes-rpc13	Service - rpcbind
32776	tcp	sometimes-rpc15	Service - rpcbind
32777	tcp	sometimes-rpc17	Service - rpcbind
32778	tcp	sometimes-rpc19	Service - rpcbind
32779	tcp	sometimes-rpc21	Service - sometimes-rpc2
32797	tcp	unknown	Service - rpcbind
35599	tcp	unknown	Service - rpcbind

192.168.235.60 : Vulnerabilities

Open X11 Server

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0526

Port/Protocol: 6000/TCP

Other References:

Nessus NASL ID : 19948
CVE ID: 1999-0526

Issue Description:

The remote X11 server accepts connection from anywhere. An attacker may connect to it to eavesdrop on the keyboard and mouse events of a user on the remote host. It is even possible for an attacker to grab a screenshot of the remote host or to display arbitrary programs.

An attacker may exploit this flaw to obtain the username and password of a user on the remote host.

Suggestions:

Restrict access to this port by using the 'xhost' command. If the X11 client/server facility is not used, disable TCP entirely.

SNMP Weak / Guessable Community String

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-2001-0514, CVE-2002-0109, CVE-2004-0311, CVE-2004-1473, CVE-2004-1474

Port/Protocol: 161/UDP

Other References:

Nessus NASL ID : 10264
Bugtraq ID: 11237, 2112, 9681, 6825, 177, 10576, 7081, 7212, 7317, 986

192.168.235.60 : Vulnerabilities

CERT VU: 329230
CVE ID: 1999-0517, 2004-0311, 1999-0254, 1999-0516, 1999-0186, 2004-1473
Generic Exploit URL: http://packetstormsecurity.nl/0402-exploits/apc_9606_backdoor.txt
Generic Informational URL: http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Guessable_Read_Community.html&fact_color=doc&tag=
Generic Informational URL: http://www.securiteam.com/exploits/Patrol_s_SNMP_Agent_3_2_can_lead_to_root_compromise.html
Generic Informational URL: http://www.securiteam.com/exploits/Windows_NT_s_SNMP_service_vulnerability.html
ISS X-Force ID: 1240, 15238, 1387, 1241, 1385, 17470
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0460.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0517.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-02/0527.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2004-09/0278.html
Microsoft Knowledge Base Article: 99880
Other Advisory URL: http://cert.uni-stuttgart.de/archive/bugtraq/1998/11/msg00249.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/advise12
Related OSVDB ID: 10204, 10206
Secunia Advisory ID: 10905, 12635
Security Tracker: 1011388, 1011389
Snort Signature ID: 1411, 1412, 1413, 1414, 1892, 1893, 2406
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-22-00178-1&searchclause=00178
Vendor Specific Advisory URL: http://www.auscert.org.au/render.html?it=494
Vendor Specific Advisory URL: http://www.sarc.com/avcenter/security/Content/2004.09.22.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1582
Vendor Specific Solution URL: http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch
Vendor Specific Solution URL: http://www.sun.com/solstice/products/ent.agents/
Vendor URL: http://www.apcc.com/
Vendor URL: http://www.managementsoftware.hp.com/
Vendor URL: http://www.symantec.com/

Issue Description:

The SNMP community string on the remote host is still set to the default or can easily be guessed.

Simple Network Management Protocol (SNMP) is used to remotely manage or monitor a host or network device. If an attacker is able to guess the read community string, an attacker will be able to freely view information like the operating system version, IP addresses, interfaces, processes/services, usernames, shares, etc. If the write community string is guessable an attacker has the ability to change system information, leading to anything from a partial to full compromise of the remote host.

Raw Scanner Output:

Plugin output :
The remote SNMP server replies to the following default community strings :
- public

192.168.235.60 : Vulnerabilities

Suggestions:

SNMP should preferably be removed if not in use.;;
Alternatively, the following security precautions should be put in place:;
- All community strings should be set to stronger, less easily guessable alternatives.;
- If SNMP is only used for monitoring purposes, write access should be disabled.;
- SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).;
- Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;;
For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:;
Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;

X Display Manager Control Protocol (XDMCP)

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 177/UDP

Other References:

Nessus NASL ID : 10891

Issue Description:

XDMCP allow a Unix user to remotely obtain a graphical X11 login
(and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.
Note that XDMCP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimates users by impersonating the XDMCP server. In addition to this, XDMCP is not a ciphered protocol which make it easy for an attacker to capture the keystrokes entered by the user.

Suggestions:

Disable the XDMCP if you do not use it, and do not allow this service to run across the Internet

Dangerous Service: rlogin

192.168.235.60 : Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-1999-0651

Port/Protocol: 513/TCP

Other References:

Nessus NASL ID : 10205

Issue Description:

The remote host is running the 'rlogin' service, a remote login daemon which allows people to log in this host and obtain an
interactive shell.

This service is dangerous because it is not ciphered - that is everyone can sniff the data that passes between the rlogin client and the rlogin server. This includes logins and passwords.

Suggestions:

You should disable this service in /etc/inetd.conf.

Unencrypted Telnet Server

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 42263

Issue Description:

The remote Telnet server transmits traffic in cleartext.

The remote host is running a Telnet server over an unencrypted channel.
Using Telnet over an unencrypted channel is not recommended as logins, passwords and commands are transferred in cleartext. An attacker may eavesdrop on a Telnet session and obtain credentials or other sensitive information.
Use of SSH is prefered nowadays as it protects credentials from eavesdropping and can tunnel additional

192.168.235.60 : Vulnerabilities

data streams such as the X11 session.

Suggestions:

Disable this service and use SSH instead.

Comments:

Created On: 2009-12-22 12:38:14
Moderated to impact: medium
This issue rating was escalated due to the dangers associated with clear text authentication across open networks such as the Internet.

Administrative Directories

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95251

Issue Description:

Administrative directories were discovered within your web application during a Directory Enumeration scan. Risks associated with an attacker discovering an administrative directory on your application server typically include the potential for the attacker to use the administrative applications to affect the operations of the web site.

The primary danger from an attacker finding a publicly available directory on your web application server depends on what type of directory it is, and what files it contains. Administrative directories typically contain applications capable of changing the configuration of the running software; an attacker who gains access to an administrative application can drastically affect the operation of the web site.

Raw Scanner Output:

http://192.168.235.60:6788/manager/

Suggestions:

Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

192.168.235.60 : Vulnerabilities

FTP Supports Clear Text Authentication

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 34324

Issue Description:

The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

Suggestions:

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.

Comments:

Created On: 2009-12-22 12:35:24
Moderated to impact: medium
This issue rating has been increased taking into account the dangers associated with allowing clear text authentication across open networks such as the Internet.

Directory Listing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95115
Apache:
http://httpd.apache.org/docs/misc/security_tips.html
http://www.w3.org/Security/faq/wwwsf3.html
http://linux.omnipotent.net/article.php?article_id=3667

192.168.235.60 : Vulnerabilities

IIS:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/iis/default.mspx
Netscape:
http://www.belk.com/manual/ag/esaccess.htm

Issue Description:

A serious Directory Listing vulnerability was discovered within the web application.
Risks associated with an attacker discovering a Directory Listing, which is a complete index of all of the resources located in that directory, result from the fact that files that should remain hidden, such as data files, backed-up source code, or applications in development, may then be visible. The specific risks depend upon the specific files that are listed and accessible.

Risks associated with an attacker discovering a Directory Listing on your application server depend upon what type of directory is discovered, and what types of files are contained within it.
The primary threat from an accessible Directory Listing is that hidden files such as data files, source code, or applications under development will then be visible to a potential attacker. In addition to accessing files containing sensitive information, other risks include an attacker utilizing the information discovered in that directory to perform other types of attacks.

Raw Scanner Output:

http://192.168.235.60:6788/manager/images/
http://192.168.235.60:6788/manager/
http://192.168.235.60:6788/console/faces/com_sun_web_ui/help/

Suggestions:

Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application.
i) Restrict access to important files or directories only to those who actually need it.
ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.

SSL Certificate Signed using Weak Hashing Algorithm

Impact: Level 3 - High

CVE Reference: CVE-2004-2761

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 35291

192.168.235.60 : Vulnerabilities

http://tools.ietf.org/html/rfc3279
http://www.phreedom.org/research/rogue-ca/
http://www.microsoft.com/technet/security/advisory/961509.mspx http://www.kb.cert.org/vuls/id/836068

Issue Description:

The remote service uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5.

These algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow him to masquerade as the affected service.

Suggestions:

Contact the Certificate Authority to have the certificate reissued.

TCP Sequence Number Approximation

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-0230

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 12213
Bugtraq ID: 10183
CERT VU: 415294
CERT: CA-2001-09, TA04-111A
CVE ID: 2004-0230
FrSIRT Advisory: ADV-2006-3983
Generic Exploit URL: http://www.osvdb.org/ref/04/04030-exploit.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/disconn.py
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/Kreset.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp_rfc31337-compliant.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/tcp_reset.c
Generic Exploit URL: http://www.packetstormsecurity.org/0405-exploits/autoRST.c
Generic Exploit URL: http://www.packetstormsecurity.org/cisco/ttt-1.3r.tar.gz
Generic Informational URL: http://nytimes.com/aponline/technology/AP-Internet -Threat.html
Generic Informational URL:

192.168.235.60 : Vulnerabilities

http://slashdot.org/articles/04/04/20/1738217.shtml?tid=126&tid=128&tid=172&tid=95
Generic Informational URL: http://www.cnn.com/2004/TECH/internet/04/20/internet.threat/index.html
Generic Informational URL: http://www.eweek.com/article2/0,1759,1571185,00.asp
Generic Informational URL: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
Generic Informational URL: http://www.ietf.org/rfc/rfc0793.txt
Generic Informational URL: http://www.msnbc.msn.com/id/4788445/
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.ppt
ISS X-Force ID: 15886
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0028.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0029.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108302060014745&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108506952116653&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
Microsoft Knowledge Base Article: 922819
Microsoft Security Bulletin: MS05-019
Microsoft Security Bulletin: MS06-064
Other Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3/SCOSA-2005.3.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9/SCOSA-2005.9.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Other Advisory URL: http://www.jpcert.or.jp/at/2004/at040003.txt
Other Advisory URL: http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx
Other Advisory URL: http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
Other Advisory URL: http://www.seil.jp/en/ann/announce_en_20040421_01.txt
Other Advisory URL: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Other Advisory URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/170
Other Solution URL: http://isc.sans.org/diary.php?date=2004-04-20
OVAL ID: 4791, 2689, 3508, 270
Related OSVDB ID: 6094, 29429, 4030
Secunia Advisory ID: 11448, 11447, 11443, 11444, 11445, 11462, 11458, 11682, 11679, 12682, 14946, 22341, 14170, 11440
Snort Signature ID: 2523
US-CERT Cyber Security Alert: TA04-111A
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2005.05.02.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
Vendor Specific Advisory URL: http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
Vendor Specific Advisory URL: http://www.juniper.net/support/alert.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/niscc-236929.txt
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1535

192.168.235.60 : Vulnerabilities

Vendor Specific Advisory URL: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
Vendor Specific News/Changelog Entry: http://www.juniper.net/support/alert.html
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc

Issue Description:

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc.).

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks.

Suggestions:

Please see http://www.securityfocus.com/bid/10183/solution, for the right solution for your infrastructure.

SSL Medium Strength Cipher Suites Supported

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 42873

Issue Description:

The remote service supports the use of medium strength SSL ciphers.

The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Raw Scanner Output:

Plugin output :
Here are the medium strength SSL ciphers supported by the remote server :
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv3

192.168.235.60 : Vulnerabilities

```
    EDH-RSA-DES-CBC-SHA      Kx=DH       Au=RSA    Enc=DES(56)
Mac=SHA1
    DES-CBC-SHA              Kx=RSA      Au=RSA    Enc=DES(56)
Mac=SHA1
  TLSv1
    EDH-RSA-DES-CBC-SHA      Kx=DH       Au=RSA    Enc=DES(56)
Mac=SHA1
    DES-CBC-SHA              Kx=RSA      Au=RSA    Enc=DES(56)
Mac=SHA1
The fields above are :
 {OpenSSL ciphername}
 Kx={key exchange}
 Au={authentication}
 Enc={symmetric encryption method}
 Mac={message authentication code}
 {export flag}
```

Suggestions:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Administrative Directories

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95251

Issue Description:

Administrative directories were discovered within your web application during a Directory Enumeration scan. Risks associated with an attacker discovering an administrative directory on your application server typically include the potential for the attacker to use the administrative applications to affect the operations of the web site.

The primary danger from an attacker finding a publicly available directory on your web application server depends on what type of directory it is, and what files it contains. Administrative directories typically contain applications capable of changing the configuration of the running software; an attacker who gains access to an administrative application can drastically affect the operation of the web site.

Raw Scanner Output:

192.168.235.60 : Vulnerabilities

http://192.168.235.60:6789/manager/

Suggestions:

Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

Finger zero at host Information Disclosure Vulnerability

Impact: Level 3 - High

CVSS Score: 10

CVE Reference: CVE-1999-0197

Port/Protocol: 79/TCP

Other References:

Nessus NASL ID : 10069

Issue Description:

The remote service is prone to information disclosure.

The remote host is running a 'finger' service that suffers from an information disclosure vulnerability. Specifically, it allows an unauthenticated attacker to display a list of accounts on the remote host that have never been used. This list can help an attacker to guess the operating system type and also focus his attacks.

Suggestions:

Filter access to this port, upgrade the finger server, or disable it entirely.

Directory Listing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

192.168.235.60 : Vulnerabilities

Other References:

Nessus NASL ID : 95115
Apache:
http://httpd.apache.org/docs/misc/security_tips.html
http://www.w3.org/Security/faq/wwwsf3.html
http://linux.omnipotent.net/article.php?article_id=3667
IIS:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/iis/default.mspx
Netscape:
http://www.belk.com/manual/ag/esaccess.htm

Issue Description:

A serious Directory Listing vulnerability was discovered within the web application.
Risks associated with an attacker discovering a Directory Listing, which is a complete index of all of the resources located in that directory, result from the fact that files that should remain hidden, such as data files, backed-up source code, or applications in development, may then be visible. The specific risks depend upon the specific files that are listed and accessible.

Risks associated with an attacker discovering a Directory Listing on your application server depend upon what type of directory is discovered, and what types of files are contained within it.
The primary threat from an accessible Directory Listing is that hidden files such as data files, source code, or applications under development will then be visible to a potential attacker. In addition to accessing files containing sensitive information, other risks include an attacker utilizing the information discovered in that directory to perform other types of attacks.

Raw Scanner Output:

http://192.168.235.60:6789/manager/images/
http://192.168.235.60:6789/manager/
http://192.168.235.60:6789/console/faces/com_sun_web_ui/help/

Suggestions:

Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application.
i) Restrict access to important files or directories only to those who actually need it.
ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.

Global User List

Impact: Level 3 - High

192.168.235.60 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95182

Issue Description:

This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

Raw Scanner Output:

User Name
adm
daemon
bin
sys
lp
uucp
nuucp
listen
nobody
noaccess
nobody4
gdm
postgres
root

Suggestions:

To prevent your host from being attacked, do one or more of the following:
Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

EXPN and VRFY commands

Impact: Level 3 - High

192.168.235.60 : Vulnerabilities

CVE Reference: CVE-1999-0531

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 10249

Issue Description:

The remote SMTP server answers to the EXPN and/or VRFY commands. The EXPN command can be used to find the delivery adress of mail aliases or even the full name of the recipients and the VRFY command may be used to check the validity of an account.

Your mailer should not allow remote users to use any of these commands because it gives them too much information.

Raw Scanner Output:

Plugin output :
EXPN root produces the following output :
250 2.1.5 Super-User <root@sunnyjim.asv.asv>
VRFY root produces the following output :
250 2.1.5 Super-User <root@sunnyjim.asv.asv>

Suggestions:

EXPN and VRFY should be disabled on the mail server.

Weak Supported SSL Ciphers Suites

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 26928
The following links detail how to change the supported SSL Cipher Suites for IIS:;;
How to control the ciphers for SSL and TLS;
----------;
http://support.microsoft.com/kb/216482;;
How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll;
----------;

192.168.235.60 : Vulnerabilities

http://support.microsoft.com/kb/245030;;
How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services;
----------;
http://support.microsoft.com/kb/187498;;
Apache;
----------;
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite;;
IBM HTTP Server;
----------;
ftp://ftp.software.ibm.com/software/webserver/appserv/library/v60/ihs_60.pdf;;
iPlanet;
----------;
http://docs.sun.com/source/816-5682-10/esecurty.htm#1008479;;
Note: It must be noted that these changes have not been tested by
SensePost, so the impact of these changes is unknown. The possibility exists that older Internet Browsing software may not be able to access the SSL protected portions of these websites, should they not have support for certain ciphers.;

Issue Description:

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Weaker cyphers have a higher possibility of being cracked and as such it is recommended that 128bit cyphers be used, at a minimum.

Raw Scanner Output:

Plugin output :
Here is the list of weak SSL ciphers supported by the remote server :
Low Strength Ciphers (< 56-bit key)
SSLv3
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40)
Mac=MD5 export
TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40)
Mac=MD5 export
The fields above are :
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}

192.168.235.60 : Vulnerabilities

Mac={message authentication code}
{export flag}

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

Hidden RPC Services

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 95171

Issue Description:

The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.
When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

Raw Scanner Output:

Name: status
Program: 100024
Version: 1
Protocol: tcp
Port: 32771
Name: ttdbserver
Program: 100083
Version: 1
Protocol: tcp
Port: 32775
Name: portmap/rpcbind

192.168.235.60 : Vulnerabilities

Program: 100000
Version: 2-4
Protocol: tcp
Port: 111
Name: nlockmgr
Program: 100021
Version: 1-4
Protocol: tcp
Port: 4045
Name: status
Program: 100024
Version: 1
Protocol: udp
Port: 32772
Name: rstatd
Program: 100001
Version: 2-4
Protocol: udp
Port: 32775
Name: rusersd
Program: 100002
Version: 2-3
Protocol: udp
Port: 32777

Suggestions:

Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

Dangerous Service: rsh

Impact: Level 3 - High

CVSS Score: 7.5

CVE Reference: CVE-1999-0651

Port/Protocol: 514/TCP

Other References:

Nessus NASL ID : 10245

Issue Description:

192.168.235.60 : Vulnerabilities

The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. It is a built-in backdoor into a system that an attacker will make easy use of.

Suggestions:

You should disable this service and use ssh instead.
To disable the service comment out the 'rsh' line in /etc/inetd.conf.

Self-signed certificate

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95138

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers. By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

Web Server Uses Basic Authentication

192.168.235.60 : Vulnerabilities

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 34850

Issue Description:

The remote web server contains web pages that are protected by 'Basic' authentication over plain text.
An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Raw Scanner Output:

Plugin output :
The following pages are protected.
/manager/html:/ realm="Tomcat Manager Application"

Suggestions:

Ensure that HTTP authentication is transmitted over HTTPS.

SSL Certificate - Signature Verification Failed Vulnerability

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95242

Issue Description:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

192.168.235.60 : Vulnerabilities

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

Suggestions:

Please install a server certificate signed by a trusted third-party Certificate Authority.

X Server Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6000/TCP

Other References:

Nessus NASL ID : 10407

Issue Description:

An X11 server is listening on the remote host.

This allows a cracker to make a client connect to the X server to record the keystrokes of the user which may contain sensitive information such as accounts passwords.

Suggestions:

Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

192.168.235.60 : Vulnerabilities

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

Finger redirection check

Impact: Level 2 - Medium

CVSS Score: 2.1

CVE Reference: CVE-1999-0105, CVE-1999-0106

Port/Protocol: 79/TCP

Other References:

Nessus NASL ID : 10073

Issue Description:

The remote finger service accepts redirect requests.

That is, users can perform requests like this:;
finger user@host@victim;
This allows an attacker to use this computer as a relay to gather information on a third-party network.;

192.168.235.60 : Vulnerabilities

Suggestions:

Disable the remote finger daemon (comment out the "finger" line in "/etc/inetd.conf" and restart the inetd process) or upgrade it to a more secure one.

SSH Protocol Versions Supported.

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
 - 1.99
 - 2.0
SSHv2 host key fingerprint :
ef:7b:76:da:ee:a3:ea:24:2d:9a:7d:2b:6b:a1:ac:e9

Suggestions:

Informational plugin.

CN does not match hostname

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

192.168.235.60 : Vulnerabilities

Nessus NASL ID : 95137

FTP Server type and version

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 10092

Issue Description:

The login banner gives potential attackers additional information about the system they are attacking.

Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
The remote FTP banner is :
220 sunnyjim FTP server ready.

Suggestions:

Informational plugin.

Apache Tomcat Default Error Page Version Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 39446
http://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6
http://jcp.org/en/jsr/detail?id=315

192.168.235.60 : Vulnerabilities

Issue Description:

The remote web server reports its version number on error pages.

Apache Tomcat appears to be running on the remote host and reporting its version number on the default error pages. A remote attacker could use this information to mount further attacks.

Raw Scanner Output:

Plugin output :
Nessus detected the following version number on an Apache Tomcat
404 page :
5.0.30

Suggestions:

Replace the default error pages with custom error pages to hide
the version number. Refer to the Apache wiki or the Java Servlet
Specification for more information.

X Font Service Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 7100/TCP

Other References:

Nessus NASL ID : 26971
http://www.x.org/docs/FSProtocol/fsproto.pdf
http://en.wikipedia.org/wiki/X_Font_Server

Issue Description:

The remote service is an X Window Font Service (xfs) daemon, which serves font files to clients.

Suggestions:

Limit incoming traffic to this port if desired or disable the service as the use of server-supplied fonts
is currently deprecated.

Telnet Service and Version

192.168.235.60 : Vulnerabilities

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 10281

Issue Description:

This detects the Telnet server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and types should be omitted where possible.

Raw Scanner Output:

Plugin output :
Here is the banner from the remote Telnet server :
---------- snip ----------
login:
---------- snip ----------

Suggestions:

Informational plugin.

Valid Logins Guessed with SMTP EXPN Command

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 587/TCP

Other References:

Nessus NASL ID : 95239

Issue Description:

Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity

192.168.235.60 : Vulnerabilities

of the destination user on the remote host by using the EXPN command.

If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

Raw Scanner Output:

user "root" expanded to: 2.1.5 Super-User <root@sunnyjim.asv.asv>

Suggestions:

Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

rquotad RPC Service Present

Impact: Level 2 - Medium

CVSS Score: 0

CVE Reference: CVE-1999-0625

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95150

Issue Description:

The rpc.rquotad service is running on your server. No known vulnerabilities exist for this service; however, it is highly sensitive. Therefore, unless it is required, you should disable this service.

If an unauthorized user finds a vulnerability in this daemon, then it would leave an open door into the server.

Suggestions:

If the "rquotad" RPC service is not required, then you should disable it.

Valid Logins Guessed with SMTP EXPN Command

Impact: Level 2 - Medium

192.168.235.60 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 95239

Issue Description:

Simple Mail Transfer Protocol (SMTP) is used to transfer mail between servers. When one mail server establishes a connection with another mail server to deliver an e-mail message, it can check the validity of the destination user on the remote host by using the EXPN command.

If a host is running an SMTP server, unauthorized users can obtain valid logins by brute forcing common "login names" with the EXPN command.

Raw Scanner Output:

user "root" expanded to: 2.1.5 Super-User <root@sunnyjim.asv.asv>

Suggestions:

Your mail server should not allow remote users to verify the existence of a particular user on your system. If you are using Sendmail Version 8, then you can disable the EXPN command by adding the line "noexpn" to your sendmail.cf file, which is usually located in the /etc directory.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32776/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :

192.168.235.60 : Vulnerabilities

The following RPC services are available on UDP port 32776 :
- program: 100068 (cmsd), version: 2
- program: 100068 (cmsd), version: 3
- program: 100068 (cmsd), version: 4
- program: 100068 (cmsd), version: 5

Suggestions:

Informational plugin.

Dangerous Service: rusersd

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0626

Port/Protocol: 32777/TCP

Other References:

Nessus NASL ID : 11058
CVE ID: 1999-0626
ISS X-Force ID: 183
Snort Signature ID: 584, 612, 1271

Issue Description:

The rusersd RPC service is running. It provides an attacker interesting information such as how often the system is being used, the names of the users, and more.

Suggestions:

Disable this service if not needed.

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

192.168.235.60 : Vulnerabilities

Other References:

Nessus NASL ID : 11936

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : Solaris 10
Confidence Level : 95
Method : SSH
The remote host is running Solaris 10

Suggestions:

Informational plugin.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :

192.168.235.60 : Vulnerabilities

Coyote HTTP/1.1 Connector

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32776/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32776 :
- program: 100002 (rusersd), version: 2
- program: 100002 (rusersd), version: 3

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32797/TCP

Other References:

Nessus NASL ID : 11111

192.168.235.60 : Vulnerabilities

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32797 :
- program: 1289637086 (dtcm), version: 5
- program: 1289637086 (dtcm), version: 1

Suggestions:

Informational plugin.

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32771/TCP

Other References:

192.168.235.60 : Vulnerabilities

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32771 :
- program: 100024 (status), version: 1
- program: 100133 (nsm_addrand), version: 1

Suggestions:

Informational plugin.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet:
RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

SSL Certificate Information

192.168.235.60 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 10863

Issue Description:

The scanner was able to determine what SSL ciphers are supported by the server.

The use of weak ciphers may lead to the compromise of data in transit.

Raw Scanner Output:

Plugin output :
Subject Name:
Country: US
State/Province: Mass
Locality: Burlington
Organization: Sun Microsystems
Organization Unit: Solaris Management Products and Tools
Common Name: solaris
Issuer Name:
Country: US
State/Province: Mass
Locality: Burlington
Organization: Sun Microsystems
Organization Unit: Solaris Management Products and Tools
Common Name: solaris
Serial Number: 48 D3 FE F6
Version: 1
Signature Algorithm: MD5 With RSA Encryption
Not Valid Before: Sep 19 19:35:18 2008 GMT
Not Valid After: Mar 12 19:35:18 2014 GMT
Public Key Info:
Algorithm: RSA Encryption
Public Key: 00 A5 9E AD 89 EE 69 53 6B 21 1C A0 AB 7E E4 F5 5F 4D B2 6C
99 B6 05 ED 52 47 8E 32 C5 A8 9A 08 E2 F5 86 E3 34 F6 7E F3
F8 27 82 44 27 67 2B E6 4F B1 11 39 2C A3 F3 EE 0D 5B F4 C6
4D E8 8D EC 8A 8C 46 11 91 B2 26 7E 51 A9 B2 9A 6E 53 DC DB
91 FB 75 AC F6 27 B1 29 F3 9D 8A 28 3F 2D E6 EC 5A 7F 8D B1
61 43 69 CA 2E 8D 49 34 DB 17 92 05 30 2A 53 21 5B DE AF EC
53 68 BC 12 5E B5 63 C7 7B
Exponent: 01 00 01
Signature: 00 91 24 DE B6 63 FE D9 54 18 6A BA B7 21 73 F5 77 53 D4 0C

192.168.235.60 : Vulnerabilities

DE FE C2 09 22 84 78 02 87 AA 7E 68 E6 2D 9F 2D E7 89 A0 74
30 5B F1 ED D1 B6 F7 98 89 F8 E1 39 F9 FB 30 C4 B5 37 1B DE
03 05 BB 1E 80 0D EE F4 1B 3F A1 F1 55 8C CC 3F FC 1A 1C 1F
C7 A0 3F 8B 21 97 9E 9B DB 05 6A 79 5B A5 2B E6 09 FA E1 5E
7E D6 78 4A 2B AA BE 12 DC 6E 4D 10 E8 91 A8 DD 2C 67 34 62
90 5F 92 AB 0E 7B 5B FC 48

Suggestions:

Informational plugin.

ICMP netmask request

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10113
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host is affected by an information disclosure vulnerability.

An attacker can use this information tounderstand how your network is set up and how the routing is done.
This may help him to bypass your filters.

Suggestions:

Reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17.

Protected web pages

Impact: Level 1 - Low

192.168.235.60 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 40665

Issue Description:

Some web pages needs authentication.

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :
- Basic is the simplest but the credential are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

Raw Scanner Output:

Plugin output :
The following pages are protected by the Basic authentication scheme :
/manager/html

Suggestions:

Informational plugin

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32775/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

192.168.235.60 : Vulnerabilities

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32775 :
- program: 100083 (ttdbserverd), version: 1

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 4045/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 4045 :
- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 2
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.60 : Vulnerabilities

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port through TLSv1.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32782/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32782 :
- program: 300598 (dmispd), version: 1
- program: 805306368 (dmispd), version: 1

Suggestions:

Informational plugin.

192.168.235.60 : Vulnerabilities

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 79/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A finger daemon is running on this port.

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and

whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-2.0-Sun_SSH_1.1
SSH supported authentication : gssapi-keyex,gssapi-with-mic,publickey,password,keyboard-interactive

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

192.168.235.60 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32778/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32778 :
- program: 100249 (snmpXdmid), version: 1

Suggestions:

Informational plugin.

Dangerous Service: rstatd

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0624

Port/Protocol: 32775/UDP

Other References:

Nessus NASL ID : 10227
IIS: http://xforce.iss.net/xforce/xfdb/115, 116
CVE ID: 1999-0624

Issue Description:

The rpc.rstatd service was found. The rstat daemon gives an attacker information about the host, including when the computer was last booted, how much CPU it is using, how many disks it has, and how many packets have reached it.

The service provides an attacker interesting information on:
- the CPU usage

192.168.235.60 : Vulnerabilities

- the system uptime
- its network usage
- and more

Suggestions:

Should the rpc.rstatd service not a business requirement, disable it by commenting it out of the inetd.conf file or the appropriate RC file.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
Location: http://192.168.235.60/console/faces/jsp/login/BeginLogin.jsp
Content-Length: 0
Date: Mon, 07 Dec 2009 18:24:49 GMT
Server: Apache-Coyote/1.1
Connection: close

Suggestions:

192.168.235.60 : Vulnerabilities

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32783/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32783 :
 - program: 100249 (snmpXdmid), version: 1

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 21/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

192.168.235.60 : Vulnerabilities

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An FTP server is running on this port.

Suggestions:

Informational plugin.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/manager
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
The following directories require authentication:
/manager/html

Suggestions:

It should be verified that no directories found, include sensitive information.

192.168.235.60 : Vulnerabilities

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32777/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32777 :
- program: 300598 (dmispd), version: 1
- program: 805306368 (dmispd), version: 1

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32777/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

192.168.235.60 : Vulnerabilities

Plugin output :
The following RPC services are available on UDP port 32777 :
 - program: 100002 (rusersd), version: 2
 - program: 100002 (rusersd), version: 3

Suggestions:

Informational plugin.

SMTP Server type and version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 587/TCP

Other References:

Nessus NASL ID : 10263

Issue Description:

The SMTP Server's type and version can be detected by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
Remote SMTP server banner :
220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7
 Mon, 7 Dec 2009 12:14:43 -0500 (EST)

Suggestions:

Informational plugin.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.60 : Vulnerabilities

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Coyote HTTP/1.1 Connector

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32772/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 32772 :
 - program: 1073741824 (fmproduct), version: 1

Suggestions:

Informational plugin.

192.168.235.60 : Vulnerabilities

SMTP server fingerprinting

Impact: Level 1 - Low

CVE Reference: CAN-2003-0172

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 11421

Issue Description:

Smtpscan is a SMTP fingerprinting tool. It identifies the remote mail server even if the banners were changed.

Although the banner might have been changed, smtpscan might be able to fingerprint the version number and type.

Raw Scanner Output:

Plugin output :
This server could be fingerprinted as :
Sendmail 8.12.2

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

192.168.235.60 : Vulnerabilities

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to
192.168.235.60 :
69.164.210.215
207.192.75.2
209.123.10.29
209.123.10.26
209.123.10.78
213.200.73.121
89.149.187.74
4.68.110.77
4.68.16.126
4.69.134.117
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.60

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and

192.168.235.60 : Vulnerabilities

whether the port is SSL-related or not.

Raw Scanner Output:

A telnet server is running on this port.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32778/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32778 :
 - program: 100011 (rquotad), version: 1

Suggestions:

Informational plugin.

SMTP server fingerprinting

Impact: Level 1 - Low

CVE Reference: CAN-2003-0172

Port/Protocol: 587/TCP

192.168.235.60 : Vulnerabilities

Other References:

Nessus NASL ID : 11421

Issue Description:

Smtpscan is a SMTP fingerprinting tool. It identifies the remote mail server even if the banners were changed.

Although the banner might have been changed, smtpscan might be able to fingerprint the version number and type.

Raw Scanner Output:

Plugin output :
This server could be fingerprinted as :
Sendmail 8.12.2

SMTP Server type and version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 10263

Issue Description:

The SMTP Server's type and version can be detected by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
Remote SMTP server banner :
220 sunnyjim.asv.asv ESMTP Sendmail 8.13.7/8.13.7
Mon, 7 Dec 2009 12:09:34 -0500 (EST)

Suggestions:

192.168.235.60 : Vulnerabilities

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 111 :
- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2

Suggestions:

Informational plugin.

Supported SSL Ciphers Suites

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 21643
http://www.openssl.org/docs/apps/ciphers.html

Issue Description:

192.168.235.60 : Vulnerabilities

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

Raw Scanner Output:

```
Plugin output :
Here is the list of SSL ciphers supported by the remote server :
  Low Strength Ciphers (< 56-bit key)
    SSLv3
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
    TLSv1
      EXP-EDH-RSA-DES-CBC-SHA    Kx=DH(512)    Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-DES-CBC-SHA          Kx=RSA(512)   Au=RSA     Enc=DES(40)
Mac=SHA1   export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA     Enc=RC4(40)
Mac=MD5    export
  Medium Strength Ciphers (>= 56-bit and < 112-bit key)
    SSLv3
      EDH-RSA-DES-CBC-SHA       Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
      DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
    TLSv1
      EDH-RSA-DES-CBC-SHA       Kx=DH        Au=RSA     Enc=DES(56)
Mac=SHA1
      DES-CBC-SHA              Kx=RSA       Au=RSA     Enc=DES(56)
Mac=SHA1
  High Strength Ciphers (>= 112-bit key)
    SSLv3
      EDH-RSA-DES-CBC3-SHA      Kx=DH        Au=RSA     Enc=3DES(168)
Mac=SHA1
      DES-CBC3-SHA             Kx=RSA       Au=RSA     Enc=3DES(168)
Mac=SHA1
      RC4-MD5                  Kx=RSA       Au=RSA     Enc=RC4(128)
Mac=MD5
      RC4-SHA                  Kx=RSA       Au=RSA     Enc=RC4(128)
Mac=SHA1
    TLSv1
      EDH-RSA-DES-CBC3-SHA      Kx=DH        Au=RSA     Enc=3DES(168)
Mac=SHA1
      DHE-RSA-AES128-SHA        Kx=DH        Au=RSA     Enc=AES(128)
Mac=SHA1
      DES-CBC3-SHA             Kx=RSA       Au=RSA     Enc=3DES(168)
Mac=SHA1
```

192.168.235.60 : Vulnerabilities

```
    AES128-SHA              Kx=RSA       Au=RSA     Enc=AES(128)
Mac=SHA1
    RC4-MD5                 Kx=RSA       Au=RSA     Enc=RC4(128)
Mac=MD5
    RC4-SHA                 Kx=RSA       Au=RSA     Enc=RC4(128)
Mac=SHA1
The fields above are :
 {OpenSSL ciphername}
 Kx={key exchange}
 Au={authentication}
 Enc={symmetric encryption method}
 Mac={message authentication code}
 {export flag}
```

Suggestions:

Reconfigure the affected application if possible to avoid use of weak ciphers.

Protected web pages

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 40665

Issue Description:

Some web pages needs authentication.

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :
- Basic is the simplest but the credential are sent in clear text.
- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.
- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

Raw Scanner Output:

Plugin output :
The following pages are protected by the Basic authentication scheme :
/manager/html

192.168.235.60 : Vulnerabilities

Suggestions:

Informational plugin

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SMTP server is running on this port.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 4045/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

192.168.235.60 : Vulnerabilities

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 4045 :
- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 2
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32775/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32775 :
- program: 100001 (rstatd), version: 2
- program: 100001 (rstatd), version: 3
- program: 100001 (rstatd), version: 4

Suggestions:

Informational plugin.

RPC Service Identification

192.168.235.60 : Vulnerabilities

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 32772/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 32772 :
- program: 100024 (status), version: 1
- program: 100133 (nsm_addrand), version: 1

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 111 :
- program: 100000 (portmapper), version: 4

192.168.235.60 : Vulnerabilities

- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2

Suggestions:

Informational plugin.

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

192.168.235.60 : Vulnerabilities

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A TLSv1 server answered on this port.

Suggestions:

Informational plugin.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
 Location: https://192.168.235.60/console/faces/jsp/login/BeginLogin.jsp
 Content-Length: 0
 Date: Mon, 07 Dec 2009 18:24:50 GMT

192.168.235.60 : Vulnerabilities

Server: Apache-Coyote/1.1
Connection: close

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 587/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SMTP server is running on this port.

Suggestions:

Informational plugin.

Dangerous Service: finger

Impact: Level 1 - Low

CVSS Score: 5

CVE Reference: CVE-1999-0612, CVE-1999-0259

192.168.235.60 : Vulnerabilities

Port/Protocol: 79/TCP

Other References:

Nessus NASL ID : 10068
CVE ID: CVE-1999-0612, CVE-1999-0259
ISS X-Force ID: 46, 48
Snort Signature ID: 324, 331, 839

Issue Description:

The finger service is running on this host.

The finger service allows an attacker to determine which users are currently connected to the host as well as the IP addresses they are connecting from. By using arpspoofing and sniffing techniques, the traffic passed from the clients to the host may be sniffed for sensitive information such as logon credentials.
Obtaining user names is the often the first step of an attack.

Suggestions:

The finger service is seldom used any more and should simply be disabled.;;
To disable the service on Cisco routers:;
a.Connect to the router and go into "enable" mode.
b.Do "configure terminal".
c.Issue the command "no ip finger".
d.To save the configuration: exit once and issue the "write" command.;;

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

192.168.235.60 : Vulnerabilities

Plugin output :
The following directories were discovered:
/manager
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
The following directories require authentication:
/manager/html

Suggestions:

It should be verified that no directories found, include sensitive information.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

RPC portmapper

Impact: Level 1 - Low

CVSS Score: 0

192.168.235.60 : Vulnerabilities

CVE Reference: CVE-1999-0632

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 10223

Issue Description:

Determines whether the remote RPC portmapper is installed or not. If it is installed then its presence will be noted as a knowledge base item and will be used by the other scripts.

Suggestions:

Informational plugin.

192.168.235.60 : Potential Vulnerabilities

Buffer Overflow in CDE Subprocess Control Service

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2001-0803

Port/Protocol: 6112/TCP

Other References:

Nessus NASL ID : 10833
Bugtraq ID: 3517
CERT VU: 72583
CERT: CA-2001-31
CVE ID: 2001-0803
Generic Exploit URL: http://www.metasploit.com
ISS X-Force ID: 7396
Other Advisory URL: http://xforce.iss.net/alerts/advise101.php
Snort Signature ID: 1398
http://www.opengroup.org/cde/;
http://www.opengroup.org/desktop/faq/;

Issue Description:

There is a remotely exploitable buffer overflow vulnerability in a library function used by the CDE Subprocess Control Service. This vulnerability could be used to crash the service or to execute arbitrary code with root privileges.

There is a remotely exploitable buffer overflow vulnerability in a shared library that is used by dtspcd. During client negotiation, dtspcd accepts a length value and subsequent data from the client without performing adequate input validation. As a result, a malicious client can manipulate data sent to dtspcd and cause a buffer overflow, potentially executing code with root privileges.

Suggestions:

Solution : See http://www.cert.org/advisories/CA-2001-31.html to determine if you are vulnerable or deactivate this service (comment out the line 'dtspc' in /etc/inetd.conf and restart the inetd process).

Solaris 10 Telnet Authentication Bypass

Impact: Level 5 - Urgent

CVSS Score: 10

192.168.235.60 : Potential Vulnerabilities

CVE Reference: CVE-2007-0882

Port/Protocol: 23/TCP

Other References:

Nessus NASL ID : 24323
http://lists.sans.org/pipermail/list/2007-February/025935.html
http://isc.sans.org/diary.html?storyid=2220

Issue Description:

The remote version of telnet does not sanitize the user-supplied
'USER' environement variable. By supplying a specially malformed
USER environment variable, an attacker may force the remote
telnet server to believe that the user has already authenticated.

This flaw allows an attacker to bypass authentication when telneting to a vulnerable machine and gain a remote shell.

Suggestions:

It is recommended that telnet not be used and instead replaced with SSH. Should SSH not be a viable option, implementing the vendor supplied patch is recommended.
The vendor supplied patches are:
120068-02 (sparc)
120069-02 (i386)

Apache Tomcat JK Web Server Connector Buffer Overflow

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95250

Issue Description:

A buffer overflow vulnerability has been found in Apache Tomcat. The vulnerability is located in the Tomcat JK Web Server Connecter in the URI handler for the mod_jk.so library in the map_uri_to_worker function of the jk_uri_worker_map.c module. A buffer overflow occurs when reading over-long URLs (more than 4095 bytes), which could be exploited to write code to the stack and launch it in the server

192.168.235.60 : Potential Vulnerabilities

context. Prior authentication is not necessary in order to exploit the bug. The bug in the Connector is fixed in Tomcat 1.2.21. Only versions 1.2.19 and 1.2.20 of the Apache Tomcat JK Web Server Connector are affected.

A remote user can execute arbitrary code on the target system.

Raw Scanner Output:

http://192.168.235.60:6789/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA

Suggestions:

Recommendations include upgrading to the latest version.

Apache Tomcat JK Web Server Connector Buffer Overflow

Impact: Level 5 - Urgent

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95250

Issue Description:

A buffer overflow vulnerability has been found in Apache Tomcat. The vulnerability is located in the Tomcat JK Web Server Connecter in the URI handler for the mod_jk.so library in the map_uri_to_worker function of the jk_uri_worker_map.c module. A buffer overflow occurs when reading over-long URLs (more than 4095 bytes), which could be exploited to write code to the stack and launch it in the server context. Prior authentication is not necessary in order to exploit the bug. The bug in the Connector is fixed in Tomcat 1.2.21. Only versions 1.2.19 and 1.2.20 of the Apache Tomcat JK Web Server Connector are affected.

A remote user can execute arbitrary code on the target system.

Raw Scanner Output:

http://192.168.235.60:6788/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA

Suggestions:

Recommendations include upgrading to the latest version.

192.168.235.60 : Potential Vulnerabilities

Sun Java Web Console Navigator Cross Site Scripting

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95179

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "navigator.jsp" file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

There are no vendor-supplied patches available at this time.

Sun Java Web Console Navigator Cross Site Scripting

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95179

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "navigator.jsp"

192.168.235.60 : Potential Vulnerabilities

file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

There are no vendor-supplied patches available at this time.

Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability

Impact: Level 4 - Critical

CVSS Score: 2.6

CVE Reference: CVE-2007-1358

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95153
Vendor Reference: http://tomcat.apache.org/security-4.html
Vendor Reference: http://tomcat.apache.org/security-5.html
Vendor Reference: http://tomcat.apache.org/security-6.html

Issue Description:

A cross-site scripting vulnerability exists in Apache Tomcat. Specifically, Web pages that display the Accept-Language header value sent by the client are susceptible to a cross-site scripting attack if they assume the Accept-Language header value conforms to RFC 2616.

This vulnerability allows remote attackers to inject arbitrary Web script or HTML via crafted "Accept-Language headers that do not conform to RFC 2616.

Suggestions:

The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

Sun Java Web Console LibWebconsole_Services.SO Remote Format String

Impact: Level 4 - Critical

192.168.235.60 : Potential Vulnerabilities

CVSS Score: 7.5

CVE Reference: CVE-2007-1681

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 25082
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102854-1
BID:23539
OSVDB:34902

Issue Description:

The remote web server is prone to a format string attack.

Suggestions:

No suggestion at this time

Sun Java Web Console masthead.jsp Cross-Site Scripting

Impact: Level 4 - Critical

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95180

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "masthead.jsp" file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

192.168.235.60 : Potential Vulnerabilities

There are no vendor-supplied patches available at this time.

Multiple Vendor CDE ToolTalk Database Server Null Write Vulnerability

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2002-0677

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95151
Bugtraq ID: 5082

Issue Description:

CDE ships with a daemon called the ToolTalk database server. The ToolTalk database server allows for programs designed for use in CDE to communicate with each other. It is enabled by default on most systems shipped with CDE.
The ToolTalk database server is vulnerable to a condition that may allow NULL words to be written to arbitrary locations in memory. The vulnerability is due to an input validation error in the _TT_ISCLOSE procedure, used by ToolTalk clients to close open ToolTalk databases.
The _TT_ISCLOSE RPC accepts a file descriptor as a parameter. This integer value is used as an index for writing to structures in server memory.
There are no checks to restrict the range of the index value. Consequently, malicious file descriptor values supplied by remote clients may cause writes to occur far beyond the table in memory. The only value written is a NULL word, limiting the consequences.
It should be noted that the only authentication required is client-supplied AUTH_UNIX credentials. AUTH_UNIX credentials may be trivially spoofed by attackers.

Exploitation of this vulnerability could allow for complex attacks, potentially resulting in remote deletion and creation of arbitrary files, or code/ command execution.

Suggestions:

Please contact your vendor for patch information.

Sun Java Web Console masthead.jsp Cross-Site Scripting

Impact: Level 4 - Critical

192.168.235.60 : Potential Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95180

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "masthead.jsp" file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

There are no vendor-supplied patches available at this time.

Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability

Impact: Level 4 - Critical

CVSS Score: 2.6

CVE Reference: CVE-2007-1358

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95153
Vendor Reference: http://tomcat.apache.org/security-4.html
Vendor Reference: http://tomcat.apache.org/security-5.html
Vendor Reference: http://tomcat.apache.org/security-6.html

Issue Description:

A cross-site scripting vulnerability exists in Apache Tomcat. Specifically, Web pages that display the Accept-Language header value sent by the client are susceptible to a cross-site scripting attack if they assume the Accept-Language header value conforms to RFC 2616.

192.168.235.60 : Potential Vulnerabilities

This vulnerability allows remote attackers to inject arbitrary Web script or HTML via crafted "Accept-Language headers that do not conform to RFC 2616.

Suggestions:

The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

Sun Java Web Console May Allow Unauthorized Redirection (243786)

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2008-5550

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95238
http://sunsolve.sun.com/search/document.do?assetkey=1-66-243786-1

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to an open redirect vulnerability in "console/faces/jsp/login/BeginLogin.jsp".
This can be exploited using the "redirect_url" parameter in a specially-crafted URL to redirect a legitinate authenticated user to arbitrary Web sites. (CVE-2008-5550)
Sun Java Web Console Versions 3.0.2 through 3.0.5 are vulnerable.

Successful exploitation of this vulnerability allows a local or remote unprivileged user to redirect a properly authenticated user to arbitrary Web sites and conduct phishing attacks.

Suggestions:

This issue has been addressed in the following releases:
SPARC Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later
Solaris 10 with patch 125952-18 or later
x86 Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later
Solaris 10 with patch 125953-18 or later
Linux Platform:

192.168.235.60 : Potential Vulnerabilities

Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later
Windows:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later
Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.

Sun Java Web Console May Allow Unauthorized Redirection (243786)

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2008-5550

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95238
http://sunsolve.sun.com/search/document.do?assetkey=1-66-243786-1

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to an open redirect vulnerability in "console/faces/jsp/login/BeginLogin.jsp".
This can be exploited using the "redirect_url" parameter in a specially-crafted URL to redirect a legitinate authenticated user to arbitrary Web sites. (CVE-2008-5550)
Sun Java Web Console Versions 3.0.2 through 3.0.5 are vulnerable.

Successful exploitation of this vulnerability allows a local or remote unprivileged user to redirect a properly authenticated user to arbitrary Web sites and conduct phishing attacks.

Suggestions:

This issue has been addressed in the following releases:
SPARC Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later
Solaris 10 with patch 125952-18 or later
x86 Platform:
Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later
Solaris 10 with patch 125953-18 or later
Linux Platform:
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later
Windows:

192.168.235.60 : Potential Vulnerabilities

Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later
Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later
Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.

Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2007-3386

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95224
BugTraq ID: 25314
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

Cross-site scripting vulnerability exists in the Host Manager Servlet for Apache Tomcat 6 and 5.

This vulnerability allows remote attackers to inject arbitrary HTML and Web script using specially crafted requests, as shown using the aliases parameter to an add action in the Host Manager Servlet.

Suggestions:

Refer to this Apache Tomcat Web site for details about the latest versions.

Apache Tomcat Information Disclosure Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2007-3382, CVE-2007-3385

Port/Protocol: 6788/TCP

Other References:

192.168.235.60 : Potential Vulnerabilities

Nessus NASL ID : 95221
BID: 25316
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

Apache Tomcat is prone to multiple information disclosure vulnerabilities because it fails to adequately sanitize user-supplied data.

Apache Tomcat treats single quotes as delimiters in cookies and does not handle the " sequence in a cookie value, which might cause sensitive session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

Suggestions:

The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2007-3386

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95224
BugTraq ID: 25314
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

Cross-site scripting vulnerability exists in the Host Manager Servlet for Apache Tomcat 6 and 5.

This vulnerability allows remote attackers to inject arbitrary HTML and Web script using specially crafted requests, as shown using the aliases parameter to an add action in the Host Manager Servlet.

Suggestions:

192.168.235.60 : Potential Vulnerabilities

Refer to this Apache Tomcat Web site for details about the latest versions.

Sendmail Long Header Denial Of Service Vulnerability

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2006-4434

Port/Protocol: 25/TCP

Other References:

Nessus NASL ID : 95061
http://www.securityfocus.com/bid/19714
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4434

Issue Description:

Sendmail is prone to a denial-of-service vulnerability.

An attacker can exploit this issue to crash the Sendmail process, causing a denial of service.

Suggestions:

Upgrade to version 8.13.8 or greater.

Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications

Impact: Level 3 - High

CVSS Score: 3.5

CVE Reference: CVE-2007-2450

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95223
Bugtraq ID: 24475
http://tomcat.apache.org/security-4.html

192.168.235.60 : Potential Vulnerabilities

http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

A cross-site scripting vulnerability exists in Apache Tomcat Versions 4, 5 and 6. This issue occurs due to an error in the Manager Web application which does not escape user-provided data before including it in the output.

Successful exploitation may allow remote authenticated users to inject arbitrary Web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

Suggestions:

Refer to this Apache Tomcat Web site for details about the latest versions.

Sun Java Web Console < 3.0.5 Remote File Enumeration

Impact: Level 3 - High

CVSS Score: 7.8

CVE Reference: CVE-2008-1286

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 31423

Issue Description:

According to its version, the installation of Sun Java Web Console on the remote host.

Which may allow a local or remote unprivileged user to determine the existence of files or directories in access restricted directories, which could result in a loss of confidentiality.

Suggestions:

Apply the appropriate patch as discussed in the vendor advisory:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-231526-1

Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications

192.168.235.60 : Potential Vulnerabilities

Impact: Level 3 - High

CVSS Score: 3.5

CVE Reference: CVE-2007-2450

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95223
Bugtraq ID: 24475
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

A cross-site scripting vulnerability exists in Apache Tomcat Versions 4, 5 and 6. This issue occurs due to an error in the Manager Web application which does not escape user-provided data before including it in the output.

Successful exploitation may allow remote authenticated users to inject arbitrary Web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

Suggestions:

Refer to this Apache Tomcat Web site for details about the latest versions.

Sun Java Web Console helpwindow.jsp Cross Site Scripting

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95237

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "helpwindow.jsp"

192.168.235.60 : Potential Vulnerabilities

file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

There are no vendor-supplied patches available at this time.

Sun Java Web Console helpwindow.jsp Cross Site Scripting

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95237

Issue Description:

Sun Java Web Console is a Web application which is used to administer Web-based Sun system management applications.
The application is prone to a cross-site scripting vulnerability due to an error in the "helpwindow.jsp" file.

An attacker could exploit this issue to perform cross-site scripting attacks on unsuspecting users in the context of the affected application. This could allow an attacker to steal cookie-based authentication credentials, which could be used to launch other attacks.

Suggestions:

There are no vendor-supplied patches available at this time.

Apache Tomcat Information Disclosure Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2007-3382, CVE-2007-3385

192.168.235.60 : Potential Vulnerabilities

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95221
BID: 25316
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

Apache Tomcat is prone to multiple information disclosure vulnerabilities because it fails to adequately sanitize user-supplied data.

Apache Tomcat treats single quotes as delimiters in cookies and does not handle the " sequence in a cookie value, which might cause sensitive session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

Suggestions:

The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.

Sun Java Web Console < 3.0.5 Remote File Enumeration

Impact: Level 3 - High

CVSS Score: 7.8

CVE Reference: CVE-2008-1286

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 31423

Issue Description:

According to its version, the installation of Sun Java Web Console on the remote host.

Which may allow a local or remote unprivileged user to determine the existence of files or directories in access restricted directories, which could result in a loss of confidentiality.

Suggestions:

192.168.235.60 : Potential Vulnerabilities

Apply the appropriate patch as discussed in the vendor advisory:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-231526-1

Apache Tomcat Multiple Content Length Headers Information Disclosure Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2005-2090

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95222
Bugtraq ID: 13873
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html

Issue Description:

This vulnerability exists in Apache Tomcat Versions 4, 5 and 6 when the server doesn't reject multiple content length header requests.

When these kinds of requests are processed by firewalls, caches, proxies and Tomcat, they may result in Web cache poisoning, XSS attack and information disclosure.

Suggestions:

Refer to this Apache Tomcat Web site for details about the latest versions.

Apache Tomcat Cross-Application File Manipulation

Impact: Level 2 - Medium

CVSS Score: 3.6

CVE Reference: CVE-2009-0783

Port/Protocol: 6789/TCP

192.168.235.60 : Potential Vulnerabilities

Other References:

Nessus NASL ID : 39479
https://issues.apache.org/bugzilla/show_bug.cgi?id=29936
http://www.securityfocus.com/archive/1/504090
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-4.html

Issue Description:

The web server running on the remote host has an information disclosure vulnerability.

According to its self-reported version number, the remote host is running a vulnerable version of Apache Tomcat. Affected versions permit a web application to replace the XML parser used to process the XML and TLD files of other applications. This could allow a malicious web app to read or modify 'web.xml', 'context.xml', or TLD files of arbitrary web applications.

Suggestions:

Upgrade to versions 6.0.20 / 5.5.SVN / 4.1.SVN or later, or apply the patches referenced in the vendor advisory.

Apache Tomcat Default Error Page Version Detection

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 39446
http://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6
http://jcp.org/en/jsr/detail?id=315

Issue Description:

The remote web server reports its version number on error pages.

Apache Tomcat appears to be running on the remote host and reporting its version number on the default error pages. A remote attacker could use this information to mount further attacks.

Raw Scanner Output:

192.168.235.60 : Potential Vulnerabilities

Plugin output :
SensePost detected the following version number on an Apache Tomcat
404 page :
5.0.30

Suggestions:

Replace the default error pages with custom error pages to hide
the version number. Refer to the Apache wiki or the Java Servlet
Specification for more information.

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Impact: Level 2 - Medium

CVSS Score: 6.4

CVE Reference: CVE-2009-3555

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 42880
http://extendedsubset.com/?p=8
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.kb.cert.org/vuls/id/120541
http://www.g-sec.lu/practicaltls.pdf
https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt
BID:36935
OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971, OSVDB:59972, OSVDB:59973, OSVDB:59974

Issue Description:

The remote service allows renegotiation of TLS / SSL connections.

Suggestions:

No suggestion at this time

Apache Tomcat Cross-Application File Manipulation

Impact: Level 2 - Medium

CVSS Score: 3.6

192.168.235.60 : Potential Vulnerabilities

CVE Reference: CVE-2009-0783

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 39479
https://issues.apache.org/bugzilla/show_bug.cgi?id=29936
http://www.securityfocus.com/archive/1/504090
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-4.html

Issue Description:

The web server running on the remote host has an information disclosure vulnerability.

According to its self-reported version number, the remote host is running a vulnerable version of Apache Tomcat. Affected versions permit a web application to replace the XML parser used to process the XML and TLD files of other applications. This could allow a malicious web app to read or modify 'web.xml', 'context.xml', or TLD files of arbitrary web applications.

Suggestions:

Upgrade to versions 6.0.20 / 5.5.SVN / 4.1.SVN or later, or apply the patches referenced in the vendor advisory.

Apache Tomcat 4 and 5 Directory Listings Information Disclosure Vulnerability

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: CVE-2006-3835

Port/Protocol: 6788/TCP

Other References:

Nessus NASL ID : 95220
BID: 19106
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html

Issue Description:

192.168.235.60 : Potential Vulnerabilities

Apache Tomcat versions from 4.0.0 to 4.0.6, 4.1.0 to 4.1.31, 5.0.0 to 5.0.30, and 5.5.0 to 5.5.12 have Directory Listings enabled by default.

A directory listing may be shown when the request contains file name preceded by a semicolon.

Suggestions:

Refer to the Apache Tomcat Web site for details on the latest versions.

Apache Tomcat 4 and 5 Directory Listings Information Disclosure Vulnerability

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: CVE-2006-3835

Port/Protocol: 6789/TCP

Other References:

Nessus NASL ID : 95220
BID: 19106
http://tomcat.apache.org/security-4.html
http://tomcat.apache.org/security-5.html

Issue Description:

Apache Tomcat versions from 4.0.0 to 4.0.6, 4.1.0 to 4.1.31, 5.0.0 to 5.0.30, and 5.5.0 to 5.5.12 have Directory Listings enabled by default.

A directory listing may be shown when the request contains file name preceded by a semicolon.

Suggestions:

Refer to the Apache Tomcat Web site for details on the latest versions.

192.168.235.61 : Overview

Host Details

DNS - Reverse Record
None
NETBIOS - Name
None
OS - OS Name
Suse Linux
PORT - Port/Protocol/Service/Banner Information
22/tcp(ssh) SSH-1.99-OpenSSH_3.6.1p1
PORT - Port/Protocol/Service/Banner Information
111/tcp(rpc-portmapper) none
PORT - Port/Protocol/Service/Banner Information
80/tcp(www) Apache 2.2.0 (Linux SUSE)

Open Ports

Port	Protocol	Service	Comment
22	tcp	ssh	Banner - SSH-1.99-OpenSSH_3.6.1p1
80	tcp	http	Banner - Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c mod_autoindex_color PHP/5.1.6
111	tcp	sunrpc	Service - RPC Portmapper
111	udp	sunrpc	Service - RPC Portmapper

192.168.235.61 : Vulnerabilities

Outdated SSH Protocol Versions Supported

Impact: Level 4 - Critical

CVE Reference: CVE-2001-0361, CVE-2001-1473 , CVE-2001-0572

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10882
Bugtraq ID: 2344
CERT VU: 61576, 997481, 888801, 161576
CIAC Advisory: I-047, m-017
CVE ID: 2001-0361, 2001-0572
Generic Informational URL: http://www.securityfocus.com/archive/1/161150
ISS X-Force ID: 6082
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2001-03/0225.html
Related OSVDB ID: 729
Snort Signature ID: 1324, 1325, 1326, 1327
Vendor Specific Advisory URL:
http://www.cisco.com/en/US/tech/tk583/tk617/technologies_security_advisory09186a00800b168e.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
Vendor Specific Advisory URL: http://www.debian.org/security/2001/dsa-027

Issue Description:

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Suggestions:

If you use OpenSSH, set the option 'Protocol' to '2'.
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.

Default Password: Guest Account

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-1999-0502, CVE-1999-0501

192.168.235.61 : Vulnerabilities

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11256
CVE ID: 1999-0502, 1999-0501
Generic Informational URL: http://www.cirt.net/cgi-bin/passwd.pl?method=showven&ven=Netscape
Generic Informational URL: http://www.sans.org/top20/#u4
Generic Informational URL: http://www.sans.org/top20/oct02.php#U10
Generic Informational URL: http://www.sans.org/top20/top10.php
Generic Informational URL: http://www.sans.org/top20/top20_oct01.php
Other Solution URL: http://www.openwall.com/john/
Snort Signature ID: 709, 710
Vendor URL: http://www.vmware.com/appliances/directory/1002

Issue Description:

The account 'guest' has the password 'guest' set.

An attacker may use it to gain further privileges on this system

Raw Scanner Output:

The account 'guest' has the password 'guest' set.
An attacker may use it to gain further privileges on this system.

Suggestions:

Set a password for this account or disable it

UDP Constant IP Identification Field Fingerprinting Vulnerability

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2002-0510

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 95152
Bugtraq ID: 4314

Issue Description:

192.168.235.61 : Vulnerabilities

The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.
Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported
that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

Suggestions:

We are not currently aware of any fixes for this issue.

Directory Listing

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95115
Apache:
http://httpd.apache.org/docs/misc/security_tips.html
http://www.w3.org/Security/faq/wwwsf3.html
http://linux.omnipotent.net/article.php?article_id=3667
IIS:
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/iis/default.mspx
Netscape:
http://www.belk.com/manual/ag/esaccess.htm

Issue Description:

A serious Directory Listing vulnerability was discovered within the web application.
Risks associated with an attacker discovering a Directory Listing, which is a complete index of all of the resources located in that directory, result from the fact that files that should remain hidden, such as data files, backed-up source code, or applications in development, may then be visible. The specific risks depend upon the specific files that are listed and accessible.

Risks associated with an attacker discovering a Directory Listing on your application server depend upon what type of directory is discovered, and what types of files are contained within it.
The primary threat from an accessible Directory Listing is that hidden files such as data files, source code, or applications under development will then be visible to a potential attacker. In addition to accessing files containing sensitive information, other risks include an attacker utilizing the

information discovered in that directory to perform other types of attacks.

Raw Scanner Output:

http://192.168.235.61:80/icons/
http://192.168.235.61:80/icons/small/

Suggestions:

Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application.
i) Restrict access to important files or directories only to those who actually need it.
ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.

Hidden RPC Services

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 95171

Issue Description:

The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a "gateway" for clients wanting to connect to any RPC daemon.
When the portmapper/rpcbind is removed or firewalled, standard RPC client programs fail to obtain the portmapper list. However, by sending carefully crafted packets, it's possible to determine which RPC programs are listening on which port. This technique is known as direct RPC scanning. It's used to bypass portmapper/rpcbind in order to find RPC programs running on a port (TCP or UDP ports). On Linux servers, RPC services are typically listening on privileged ports (below 1024), whereas on Solaris, RPC services are on temporary ports (starting with port 32700).

Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.

Raw Scanner Output:

Name: portmap/rpcbind

192.168.235.61 : Vulnerabilities

Program: 100000
Version: 2
Protocol: tcp
Port: 111

Suggestions:

Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.

HTTP TRACE/TRACK Methods Supported

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2004-2320, CVE-2005-3398, CVE-2005-3498, CVE-2007-3008

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11213
Bugtraq ID: 11604, 9561, 9506
CERT VU: 867593
CVE ID: 2005-3398, 2005-3498, 2004-2320
ISS X-Force ID: 11149, 11237, 14959
Mail List Post: http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html
Nikto Item ID: 1249, 1250
Other Advisory URL: http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
Other Advisory URL: http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
Other Advisory URL: http://en.wikipedia.org/wiki/Cross-site_tracing
Other Advisory URL: http://dev2dev.bea.com/pub/advisory/68
Related OSVDB ID: 5648, 3726
Secunia Advisory ID: 17334, 21802, 10726, 32977
Security Tracker: 1015112, 102016, 1015134, 1008866
Snort Signature ID: 2056
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1
Vendor Specific Advisory URL:
ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir5.10_docs_relnotes.pdf
Vendor Specific Advisory URL:
http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_48.00.jsp
Vendor Specific News/Changelog Entry:
https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/install/v61.Readme.html#MH01128
Vendor URL:
http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/resources/index.html

192.168.235.61 : Vulnerabilities

Vendor URL: http://www.bea.com
http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp;

Issue Description:

Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick a legitimate web user into disclosing their credentials.

Suggestions:

If you are using Apache, add the following lines for each virtual host in your configuration file:;;
RewriteEngine on;
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK);
RewriteRule .* - [F];;
If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

TCP Sequence Number Approximation

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2004-0230

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 12213
Bugtraq ID: 10183
CERT VU: 415294
CERT: CA-2001-09, TA04-111A
CVE ID: 2004-0230
FrSIRT Advisory: ADV-2006-3983
Generic Exploit URL: http://www.osvdb.org/ref/04/04030-exploit.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/bgp-dosv2.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/disconn.py
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/Kreset.pl
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset-tcp_rfc31337-compliant.c
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/reset.zip
Generic Exploit URL: http://www.packetstormsecurity.org/0404-exploits/tcp_reset.c
Generic Exploit URL: http://www.packetstormsecurity.org/0405-exploits/autoRST.c

192.168.235.61 : Vulnerabilities

Generic Exploit URL: http://www.packetstormsecurity.org/cisco/ttt-1.3r.tar.gz
Generic Informational URL: http://nytimes.com/aponline/technology/AP-Internet -Threat.html
Generic Informational URL: http://slashdot.org/articles/04/04/20/1738217.shtml?tid=126&tid=128&tid=172&tid=95
Generic Informational URL: http://www.cnn.com/2004/TECH/internet/04/20/internet.threat/index.html
Generic Informational URL: http://www.eweek.com/article2/0,1759,1571185,00.asp
Generic Informational URL: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
Generic Informational URL: http://www.ietf.org/rfc/rfc0793.txt
Generic Informational URL: http://www.msnbc.msn.com/id/4788445/
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.doc
Generic Informational URL: http://www.osvdb.org/ref/04/04030-SlippingInTheWindow_v1.0.ppt
ISS X-Force ID: 15886
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0028.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2005-02/0029.html
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108302060014745&w=2
Mail List Post: http://marc.theaimsgroup.com/?l=bugtraq&m=108506952116653&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded
Microsoft Knowledge Base Article: 922819
Microsoft Security Bulletin: MS05-019
Microsoft Security Bulletin: MS06-064
Other Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.3/SCOSA-2005.3.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9/SCOSA-2005.9.txt
Other Advisory URL: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc
Other Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Other Advisory URL: http://www.jpcert.or.jp/at/2004/at040003.txt
Other Advisory URL: http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx
Other Advisory URL: http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx
Other Advisory URL: http://www.seil.jp/en/ann/announce_en_20040421_01.txt
Other Advisory URL: http://www.uniras.gov.uk/vuls/2004/236929/index.htm
Other Advisory URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/170
Other Solution URL: http://isc.sans.org/diary.php?date=2004-04-20
OVAL ID: 4791, 2689, 3508, 270
Related OSVDB ID: 6094, 29429, 4030
Secunia Advisory ID: 11448, 11447, 11443, 11444, 11445, 11462, 11458, 11682, 11679, 12682, 14946, 22341, 14170, 11440
Snort Signature ID: 2523
US-CERT Cyber Security Alert: TA04-111A
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
Vendor Specific Advisory URL: http://securityresponse.symantec.com/avcenter/security/Content/2005.05.02.html
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2005-097_SCASA-2005-14.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_tcp_can-2004-0230.html
Vendor Specific Advisory URL: http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
Vendor Specific Advisory URL: http://www.juniper.net/support/alert.html

192.168.235.61 : Vulnerabilities

Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/niscc-236929.txt
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1535
Vendor Specific Advisory URL: http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
Vendor Specific News/Changelog Entry: http://www.juniper.net/support/alert.html
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc

Issue Description:

The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc.).

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range of the expected sequence number for a packet in the session. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks.

Suggestions:

Please see http://www.securityfocus.com/bid/10183/solution, for the right solution for your infrastructure.

TCP Packet Filtering Weakness

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11618
Bugtraq ID: 7487
CERT VU: 464113
Generic Informational URL: http://www.securityfocus.com/archive/1/296122
ISS X-Force ID: 11972
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-019.0.txt
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenLinux/
http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html

Issue Description:

192.168.235.61 : Vulnerabilities

The remote host does not discard TCP SYN packets that also have the FIN flag set.
Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules and establish a session with a service that would otherwise be inaccessible.

The behavior of this host is incorrect but is not necessarily insecure. If the host is protected by a stateless firewall that relies on the TCP flags when filtering then it may be possible for an attacker to bypass the network firewall policies by setting both the SYN and FIN flags within a malformed TCP packet. This may make it possible for an attacker to establish a session with a service that would otherwise be inaccessible.

Suggestions:

Contact your vendor for a patch.

SSH Protocol Versions Supported.

Impact: Level 2 - Medium

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10881

Issue Description:

This plugin determines which versions of the SSH protocol the remote SSH daemon supports.

Raw Scanner Output:

Plugin output :
The remote SSH daemon supports the following versions of the
SSH protocol :
- 1.33
- 1.5
- 1.99
- 2.0
SSHv1 host key fingerprint :
8a:44:8e:aa:67:c1:77:73:c3:3b:a5:9c:10:a5:65:cc
SSHv2 host key fingerprint :
6a:37:45:22:54:8d:89:d5:4f:c5:7b:e7:49:45:fb:ba

Suggestions:

Informational plugin.

192.168.235.61 : Vulnerabilities

ICMP timestamp request

Impact: Level 1 - Low

CVE Reference: CVE-1999-0524

Port/Protocol: 0/ICMP

Other References:

Nessus NASL ID : 10114
CVE ID: 1999-0524
ISS X-Force ID: 322, 8812, 306
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1434

Issue Description:

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which set on the remote host.;;
This may help him to defeat all your time based authentication protocols.;

The information gained may help an attacker in defeating time based authentification protocols.

Raw Scanner Output:

Plugin output :
The difference between the local and remote clocks is -21189 seconds.

Suggestions:

Filter out the ICMP timestamp requests (type 13), and the outgoing ICMP timestamp replies (type 14).

OS Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 11936

192.168.235.61 : Vulnerabilities

Issue Description:

This script attempts to identify the operating system type and version.

An attacker may use this to identify the kind of the remote operating system and gain further knowledge about this host.
Please refer to "Scan Results" in order to see the exact version found.

Raw Scanner Output:

Remote operating system : Linux Kernel 2.6 on SuSE Linux 10.1
Confidence Level : 95
Method : HTTP
The remote host is running Linux Kernel 2.6 on SuSE Linux 10.1

Suggestions:

Informational plugin.

RPC portmapper

Impact: Level 1 - Low

CVSS Score: 0

CVE Reference: CVE-1999-0632

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 10223

Issue Description:

Determines whether the remote RPC portmapper is installed or not. If it is installed then its presence will be noted as a knowledge base item and will be used by the other scripts.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

192.168.235.61 : Vulnerabilities

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/TCP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on TCP port 111 :
- program: 100000 (portmapper), version: 2

Suggestions:

Informational plugin.

HTTP Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 10107

Issue Description:

The HTTP Server's type and version can be obtained via the banner.

This information gives potential attackers additional information about the system they are attacking.

Raw Scanner Output:

Plugin output :
The remote web server type is :
Apache/2.2.0 (Linux/SUSE)
Solution : You can set the directive 'ServerTokens Prod' to limit

the information emanating from the server in its response headers.

Suggestions:

Informational plugin.

Virtual Directory Names Are Easily Guessable

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 11032

Issue Description:

Various common directories were found on the remote web server. This does not necessarily imply a security risk, but should be verified as sensitive information or dangerous site functionality may be exposed. Please refer to 'scan results' for more information.

Raw Scanner Output:

Plugin output :
The following directories were discovered:
/cgi-bin, /error, /icons
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
Other references : OWASP:OWASP-CM-006

Suggestions:

It should be verified that no directories found, include sensitive information.

Host Responds to TCP SYN Packet with Other Flags On with SYN ACK

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.61 : Vulnerabilities

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 95229

Issue Description:

The host responds to a TCP SYN packet with at least one of the following flags set with a SYN ACK packet: RST, FIN, ACK, FINIPSH.

This behavior in the TCP/IP implementation may allow a remote user to potentially bypass a firewall protecting the host, as some (especially stateless) firewalls may be configured to allow all TCP packets with one of these flags set (RST, FIN, ACK, FINIPSH) to go through without examining the packets' SYN flag.

Suggestions:

Many operating systems are known to have this behavior.

Traceroute

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/UDP

Other References:

Nessus NASL ID : 10287

Issue Description:

It was possible to perform a traceroute to the host.

Attackers use this information to map the network and host location.

Raw Scanner Output:

Plugin output :
For your information, here is the traceroute from 69.164.210.215 to 192.168.235.61 :
69.164.210.215
207.192.75.2
209.123.10.13
209.123.10.78

192.168.235.61 : Vulnerabilities

213.200.73.121
89.149.184.182
4.68.110.77
4.68.16.62
4.69.134.113
4.69.141.5
67.69.246.125
64.230.170.173
64.230.147.134
206.108.99.157
64.230.137.250
?
192.168.235.61

Suggestions:

Disable responses to ping requests (ICMP type 8) on the firewall from the Internet. This will block the necessary Time To Live (TTL) messages on which traceroute relies on. This should be tested to ensure it doesn't interfere with applications that rely on ICMP.

HyperText Transfer Protocol Information

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 24260

Issue Description:

This test is used to extract HTTP protocol information. The information extracted is the HTTP Header and Options.

The header can contain information such as the cookie field, server version, etc. The information is not necessarily dangerous unless there is a vulnerability associated with it.
Options can be dangerous too, if they allow an unauthorised user to abuse the methods.
This information has to be either manually verified (and given an appropriate risk rating) or will be discovered in other vulnerability tests.

Raw Scanner Output:

Plugin output :
Protocol version : HTTP/1.1

192.168.235.61 : Vulnerabilities

SSL : no
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :
Date: Sun, 12 Oct 2008 20:39:45 GMT
Server: Apache/2.2.0 (Linux/SUSE)
Last-Modified: Wed, 24 Sep 2008 06:14:21 GMT
ETag: "d0b3-77"
Accept-Ranges: bytes
Content-Length: 119
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Suggestions:

If dangerous methods are enabled, such as PUT, DELETE or even PROPFIND (giving evidence that WebDAV is enabled) then these findings can be considered risky to the host and should be removed or disabled in the web server configuration file.

SSH Server Type and Version

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 10267

Issue Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.

This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Raw Scanner Output:

Plugin output :
SSH version : SSH-1.99-OpenSSH_3.6.1p1
SSH supported authentication : publickey,password,keyboard-interactive

Suggestions:

192.168.235.61 : Vulnerabilities

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

An SSH server is running on this port.

Suggestions:

Informational plugin.

Service detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 22964

Issue Description:

This plugin performs service detection.

192.168.235.61 : Vulnerabilities

This plugin connects to every port and attempts to extract the banner of the service running on each, and whether the port is SSL-related or not.

Raw Scanner Output:

A web server is running on this port.

Suggestions:

Informational plugin.

RPC Service Identification

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 111/UDP

Other References:

Nessus NASL ID : 11111

Issue Description:

This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Raw Scanner Output:

Plugin output :
The following RPC services are available on UDP port 111 :
 - program: 100000 (portmapper), version: 2

Suggestions:

Informational plugin.

TCP timestamps

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

192.168.235.61 : Vulnerabilities

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 25220
http://www.ietf.org/rfc/rfc1323.txt

Issue Description:

The remote host implements TCP timestamps, as defined by RFC1323.

A side effect of this feature is that the uptime of the remote
host can be sometimes be computed.

Suggestions:

Informational plugin.

Linux Distribution Detection

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 18261

Issue Description:

This script extracts the banner of the remote web server and attempts to determine the Linux distribution
the remote host is running.

Raw Scanner Output:

Plugin output :
The linux distribution detected was :
 - SuSE Linux 10.1

Suggestions:

Should you not wish to display this information, edit httpd.conf and set the directive ServerTokens Prod
and restart Apache.

192.168.235.61 : Vulnerabilities

IP protocols scan

Impact: Level 1 - Low

CVE Reference: No CVE Reference At This Time

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 14788

Issue Description:

This scripts detects the protocols understood by the remote IP stack.

Suggestions:

Informational plugin.

192.168.235.61 : Potential Vulnerabilities

OpenSSH Buffer Management Vulnerability (OpenSSH < 3.7.1)

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2003-0682, CVE-2003-0693, CVE-2003-0695

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11837
Bugtraq ID: 8628
CERT VU: 333628
CERT: CA-2003-24
CIAC Advisory: N-151, o-030
CVE ID: 2003-0695, 2003-0693, 2003-0682
ISS X-Force ID: 13191, 13214
Other Advisory URL: http://archives.neohapsis.com/archives/fulldisclosure/2003-q3/3967.html
Other Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106373247528528&w=2
Other Advisory URL: http://xforce.iss.net/xforce/alerts/id/144
RedHat RHSA: RHSA-2003:279, RHSA-2003:280, RHSA-2003:222
Secunia Advisory ID: 9743, 10156, 9747, 9756, 9744, 9810, 9811
Security Tracker: 1007716
Vendor Specific Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:12.openssh.asc
Vendor Specific Advisory URL: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-012.txt.asc
Vendor Specific Advisory URL: ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-027.0.txt
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20030904-02-P.asc
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20031001-01-U.asc
Vendor Specific Advisory URL: http://cc.turbolinux.com/security/TLSA-2003-51.txt
Vendor Specific Advisory URL: http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000741
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/index.php?id=a&anuncio=000739
Vendor Specific Advisory URL: http://distro.conectiva.com/atualizacoes/index.php?id=a&anuncio=000741
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=61798
Vendor Specific Advisory URL: http://infocenter.guardiandigital.com/knowledgebase/123
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106381396120332&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106381409220492&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=bugtraq&m=106382542403716&w=2
Vendor Specific Advisory URL: http://marc.theaimsgroup.com/?l=openbsd-security-announce&m=106375582924840
Vendor Specific Advisory URL: http://security.debian.org/pool/updates/main/o/openssh-krb5/ssh-krb5_3.4p1-0woody4_hppa.deb
Vendor Specific Advisory URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56861&zone_32=category%3Asecurity

192.168.235.61 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56862&zone_32=category%3Asecurity
Vendor Specific Advisory URL: http://support.f-secure.com/enu/corporate/supportissue/ssh/comments/comments-issue-2003120401.shtml
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2003.1217.1
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1500.1
Vendor Specific Advisory URL: http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0100.1
Vendor Specific Advisory URL: http://www.bluecoat.com/downloads/support/BCS_OpenSSH_vulnerability.pdf
Vendor Specific Advisory URL: http://www.bluecoat.com/support/knowledge/advisory_openSSH_buffer_vulnerability.html
Vendor Specific Advisory URL: http://www.caldera.com/support/security/2003.html#OpenServer
Vendor Specific Advisory URL: http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml
Vendor Specific Advisory URL: http://www.debian.org/security/2003/dsa-382
Vendor Specific Advisory URL: http://www.debian.org/security/2003/dsa-383
Vendor Specific Advisory URL: http://www.foundrynet.com/solutions/advisories/openssh333628.html
Vendor Specific Advisory URL: http://www.juniper.net/support/security/alerts/openssh_1.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/engarde_advisory-3621.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/engarde_advisory-3649.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/gentoo_advisory-3629.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/immunix_advisory-3627.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/immunix_advisory-3635.html
Vendor Specific Advisory URL: http://www.linuxsecurity.com/advisories/slackware_advisory-3639.html
Vendor Specific Advisory URL: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:090-1
Vendor Specific Advisory URL: http://www.mindrot.org/pipermail/openssh-unix-announce/2003-September/000064.html
Vendor Specific Advisory URL: http://www.netscreen.com/services/security/alerts/openssh_1.jsp
Vendor Specific Advisory URL: http://www.openbsd.org/errata33.html#sshbuffer
Vendor Specific Advisory URL: http://www.openpkg.org/security/OpenPKG-SA-2003.040-openssh.html
Vendor Specific Advisory URL: http://www.openssh.com/txt/buffer.adv
Vendor Specific Advisory URL: http://www.riverstonenet.com/support/tb0265-9.html
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.368193
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.373294
Vendor Specific Advisory URL: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.374735
Vendor Specific Advisory URL: http://www.suse.com/de/security/2003_039_openssh.html
Vendor Specific Advisory URL: http://www.suse.de/de/security/2003_038_openssh.html
Vendor Specific Advisory URL: http://www.suse.de/de/security/2003_039_openssh.html
Vendor Specific Advisory URL: http://www.trustix.net/errata/misc/2003/TSL-2003-0033-openssh.asc.txt
Vendor Specific Advisory URL: http://www.trustix.org/pipermail/tsl-discuss/2003-September/007507.html
Vendor Specific Advisory URL: http://www.vmware.com/download/esx/esx152-patch5.html
Vendor Specific Advisory URL: http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1371
Vendor Specific Advisory URL: https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=3D

192.168.235.61 : Potential Vulnerabilities

Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-222.html
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-279.html
Vendor Specific Advisory URL: https://rhn.redhat.com/errata/RHSA-2003-280.html
Vendor Specific Advisory URL: https://www.ingrian.com/support/iwsc/security.php
Vendor Specific Advisory URL: https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2003-09-007&actionBtn=Search
Vendor Specific News/Changelog Entry: http://www116.nortel.com/docs/bvdoc/alteon/ssl/iSD-SSL_3.1.6.14_README.pdf
Vendor Specific Solution URL: ftp://ftp.openpkg.org/release/1.3/UPD/
Vendor Specific Solution URL: ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.24
Vendor Specific Solution URL: http://download.bluecoat.com/release/SGOS/index.html
Vendor Specific Solution URL: http://download.bluecoat.com/release/SGOS3/index.html
Vendor Specific Solution URL: http://oss.software.ibm.com/developerworks/projects/opensshi
Vendor Specific Solution URL: http://security.debian.org/pool/updates/main/o/openssh-krb5/ssh-krb5_3.4p1-0woody4_i386.deb
Vendor Specific Solution URL: http://sunsolve.sun.com/cobalt
Vendor Specific Solution URL: http://sunsolve.sun.com/patches/linux/security.html
Vendor Specific Solution URL: http://vmware-svca.www.conxion.com/secured/esx/esx-1.5.2-patch5.tar.gz
Vendor Specific Solution URL: http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
Vendor Specific Solution URL: http://www.cisco.com/tacpage/sw-center/
Vendor Specific Solution URL: http://www.cyclades.com/support/downloads.php
Vendor Specific Solution URL: http://www.f-secure.com/webclub/ssh/
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120244
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120245
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120246
Vendor Specific Solution URL: http://www.info.apple.com/kbnum/n120247
Vendor Specific Solution URL: http://www.mandrakesecure.net/en/ftp.php
Vendor Specific Solution URL: http://www.netscreen.com/cso
Vendor Specific Solution URL: http://www.riverstonenet.com/support/support_sw_download.shtml
Vendor Specific Solution URL: http://www.trustix.net/pub/Trustix/updates/
Vendor Specific Solution URL: https://www.ingrian.com/suppport
Vendor URL: http://www.openssh.com/

Issue Description:

OpenSSH's SSH Daemon prior to 3.7.1 contains buffer management errors, which depending on factors such as the underlying operating system might allow an attacker to execute arbitrary commands on this host. Other implementations sharing common origin may also have these issues.
An exploit for this issue is rumoured to exist.

Buffer management problems have been found in all versions of OpenSSH's SSH daemon which are potentially remotely exploitable. Rumours currently exist of exploits in the wild for this bug against Linux on the
intel platform. This vulnerability even extends to network devices using the OpenSSH implementation.
According to Cisco, devices currently vulnerable to the DoS condition include :
Cisco Catalyst Switching Software (CatOS)
CiscoWorks 1105 Hosting Solution Engine (HSE)
CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
Cisco SN 5428 Storage Router

Suggestions:

192.168.235.61 : Potential Vulnerabilities

This issue is resolved in OpenSSH releases 3.7.1 and later. Upgrade to latest stable release version of OpenSSH available from www.openssh.com. Manual patches for this issue are available from http://www.openssh.com/txt/buffer.adv.
For vendor specific patch information, look up the vendor in question from http://www.securityfocus.com/bid/8628/solution, or contact the vendor directly.

OpenSSH < 5.0

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2000-0999, CVE-2001-0572, CVE-2001-1029, CVE-2005-2797, CVE-2005-2798, CVE-2006-0225, CVE-2006-4924, CVE-2006-4925, CVE-2006-5051, CVE-2006-5052, CVE-2006-5229, CVE-2006-5794, CVE-2007-2243, CVE-2007-3102, CVE-2007-4752, CVE-2008-1483, CVE-2008-1657, CVE-2008-3234, CVE-2008-3259, CVE-2008-4109, CVE-2008-5161

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95134

Issue Description:

OpenSSH version is older than 5.0.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.0, is below:
CVE-2000-0999 - OpenBSD ssh Format String Privilege Escalation
CVE-2001-0572 - Cisco Devices SSH Password Length Disclosure, SSH Traffic Analysis Connection Attributes Disclosure
CVE-2001-1029 - OpenSSH on FreeBSD libutil Arbitrary File Read
CVE-2005-2797 - OpenSSH Multiple X11 Channel Forwarding Leaks
CVE-2005-2798 - OpenSSH GSSAPIAuthentication Credential Escalation
CVE-2006-0225 - OpenSSH scp Command Line Filename Processing Command Injection
CVE-2006-4924 - OpenSSH Identical Block Packet DoS
CVE-2006-4925 - OpenSSH packet.c Invalid Protocol Sequence Remote DoS
CVE-2006-5051 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2006-5052 - OpenSSH GSSAPI Authentication Abort Username Enumeration
CVE-2006-5229 - OpenSSH Username Password Complexity Account Enumeration
CVE-2006-5794 - OpenSSH Privilege Separation Monitor Weakness
CVE-2007-2243 - OpenSSH S/KEY Authentication Account Enumeration
CVE-2007-3102 - OpenSSH linux_audit_record_event Crafted Username Audit Log Injection

192.168.235.61 : Potential Vulnerabilities

CVE-2007-4752 - OpenSSH Trusted X11 Cookie Connection Policy Bypass
CVE-2008-1483 - OpenSSH X11 Forwarding Local Session Hijacking
CVE-2008-1657 - OpenSSH ~/.ssh/rc ForceCommand Bypass Arbitrary Command Execution
CVE-2008-3234 - OpenSSH on Debian sshd Crafted Username Arbitrary Remote SELinux Role Access
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
CVE-2008-4109 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2008-5161 - OpenSSH CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure, SSH Tectia Multiple Products CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: www.openssh.org

OpenSSH < 4.0

Impact: Level 5 - Urgent

CVSS Score: 10

CVE Reference: CVE-2001-0872, CVE-2001-1507, CVE-2002-0083, CVE-2002-0575, CVE-2002-0639, CVE-2002-0640, CVE-2002-0765, CVE-2003-0190, CVE-2003-0386, CVE-2003-0682, CVE-2003-0693, CVE-2003-0695, CVE-2003-0786, CVE-2003-0787, CVE-2003-1562, CVE-2004-0175, CVE-2004-1653, CVE-2004-2069, CVE-2004-2760, CVE-2005-2666, CVE-2005-2798, CVE-2006-0225, CVE-2006-0883, CVE-2006-4924, CVE-2006-5051, CVE-2006-5052, CVE-2007-2243, CVE-2007-4654, CVE-2008-3259, CVE-2008-4109

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95133

Issue Description:

OpenSSH version is older than 4.0.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 4.0, is below:
CVE-2001-0872 - OpenSSH UseLogin Environment Variable Local Command Execution
CVE-2001-1507 - OpenSSH with KerberosV Remote Authentication Bypass
CVE-2002-0083 - OpenSSH Channel Code Off by One Privilege Escalation
CVE-2002-0575 - OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
CVE-2002-0639 - OpenSSH SKEY/BSD_AUTH Challenge-Response Remote Overflow
CVE-2002-0640 - OpenSSH PAMAuthenticationViaKbdInt Challenge-Response Remote Overflow

192.168.235.61 : Potential Vulnerabilities

CVE-2002-0765 - OpenSSH YP Netgroups Authentication Bypass
CVE-2003-0190 - OpenSSH Root Login Timing Side-Channel Weakness, OpenSSH w/ PAM Username Validity Timing Attack
CVE-2003-0386 - OpenSSH Reverse DNS Lookup Bypass
CVE-2003-0682 - OpenSSH *realloc() Unspecified Memory Errors
CVE-2003-0693 - OpenSSH buffer_append_space() Heap Corruption
CVE-2003-0695 - OpenSSH Multiple Buffer Management Multiple Overflows
CVE-2003-0786 - OpenSSH SSHv1 PAM Challenge-Response Authentication Privilege Escalation
CVE-2003-0787 - OpenSSH PAM Conversation Function Stack Modification
CVE-2003-1562 - OpenSSH Root Login Timing Side-Channel Weakness, OpenSSH w/ PAM Username Validity Timing Attack
CVE-2004-0175 - OpenSSH scp Traversal Arbitrary File Overwrite
CVE-2004-1653 - OpenSSH Default Configuration Anon SSH Service Port Bounce Weakness
CVE-2004-2069 - OpenSSH Privilege Separation LoginGraceTime DoS
CVE-2004-2760 - OpenSSH sshd TCP Connection State Remote Account Enumeration
CVE-2005-2666 - Multiple SSH known_hosts Plaintext Host Disclosure
CVE-2005-2798 - OpenSSH GSSAPIAuthentication Credential Escalation
CVE-2006-0225 - OpenSSH scp Command Line Filename Processing Command Injection
CVE-2006-0883 - OpenSSH with OpenPAM Connection Saturation Forked Process Saturation DoS
CVE-2006-4924 - OpenSSH Identical Block Packet DoS
CVE-2006-5051 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
CVE-2006-5052 - OpenSSH GSSAPI Authentication Abort Username Enumeration
CVE-2007-2243 - OpenSSH S/KEY Authentication Account Enumeration
CVE-2007-4654 - Cisco WebNS SSHield w/ OpenSSH Crafted Large Packet Remote DoS
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
CVE-2008-4109 - OpenSSH Signal Handler Pre-authentication Race Condition Code Execution

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: www.openssh.org

OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities

Impact: Level 5 - Urgent

CVSS Score: 9.3

CVE Reference: CVE-2006-5051, CVE-2006-5052 , CVE-2008-4109, CVE-2006-4924

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 22466
Bugtraq ID: 20241, 20245
CVE ID: 2006-5051, 2008-4109, 2006-5052
ISS X-Force ID: 29254, 45202

192.168.235.61 : Potential Vulnerabilities

Mail List Post: http://lists.debian.org/debian-security-announce/2008/msg00227.html
Other Advisory URL: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-527.htm
Other Advisory URL: http://www-unix.globus.org/mail_archive/security-announce/2007/04/msg00000.html
Other Advisory URL: http://www.debian.org/security/2008/dsa-1638
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1189
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1212
RedHat RHSA: RHSA-2006:0697-9, RHSA-2006:0698, RHSA-2006:0697
Secunia Advisory ID: 22173, 22196, 22183, 22236, 22158, 22208, 22245, 22270, 22362, 22352, 22487, 22495, 22823, 22926, 23680, 24805, 24799, 31885, 32080, 32181, 28320
Security Tracker: 1020891
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20061001-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=305214
Vendor Specific Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00004.html
Vendor Specific Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Oct/0005.html
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-216.htm
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200611-06.xml
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:179
Vendor Specific Advisory URL: http://www.openbsd.org/errata.html#ssh
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-355-1
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-649-1
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=498678
Vendor Specific News/Changelog Entry: http://marc.theaimsgroup.com/?l=openbsd-cvs&m=115589252024127&w=2
Vendor Specific News/Changelog Entry: http://openssh.org/txt/release-4.4

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host contains a race condition that may allow an unauthenticated remote attacker to crash the service or, on portable OpenSSH, possibly execute code on the affected host.

In addition, another flaw exists that may allow an attacker to determine the validity of usernames on some platforms. Note that successful exploitation of these issues requires that GSSAPI authentication be enabled.

Suggestions:

Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org

SuSE Security Update: libapr-util1 (2009-10-11)

Impact: Level 5 - Urgent

CVSS Score: 10

192.168.235.61 : Potential Vulnerabilities

CVE Reference: CVE-2009-2412

Port/Protocol: 0/TCP

Other References:

Nessus NASL ID : 42234
https://bugzilla.novell.com/show_bug.cgi?id=529591
BID:0
(null)

Issue Description:

The remote SuSE system is missing a security patch for libapr-util1

Suggestions:

No suggestion at this time

OpenSSH Reverse DNS Lookup bypass

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2003-0386

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 11712
Bugtraq ID: 7831
CERT VU: 978316
CVE ID: 2003-0386
ISS X-Force ID: 12196
Mail List PostL http://archives.neohapsis.com/archives/bugtraq/2003-06/0038.html
RedHat RHSA: RHSA-2006:0298, RHSA-2006:0698
Secunia Advisory ID: 8974, 21129, 21262, 21724, 22196, 23680
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20060703-01-U.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=61798
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-174.htm
Vendor Specific Advisory URL:
http://www.vmware.com/support/kb/enduser/std_adp.php?p_sid=FsNALBWh&p_lva=&p_faqid=1534
Vendor Specific Advisory URL: http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html

192.168.235.61 : Potential Vulnerabilities

Issue Description:

You are running OpenSSH 3.6.1 (portable) or older. There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of the target server.

OpenSSH features a mecanism which can restrict the list of hosts a given user can log from by specifying pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network). However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mecanism.

Suggestions:

Upgrade to the latest stable release version of OpenSSH, available from http://www.openssh.org. This problem is resolved in OpenSSH 3.6.2 and later.

Apache < 2.2.9 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2007-6420, CVE-2007-6423, CVE-2008-0455, CVE-2008-0456, CVE-2008-2364, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2007-6421, CVE-2007-6422

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 33477
Bugtraq ID: 27236, 29653, 8707, 27409
CVE ID: 2007-6420, 2007-6421, 2007-6422, 2007-6423, 2008-2364
FrSIRT Advisory: ADV-2008-0048, ADV-2008-1798
ISS X-Force ID: 42987
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Other Advisory URL: HPSBUX02365 SSRT080118
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
Other Advisory URL: http://securityreason.com/securityalert/3523
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg27008517
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200803-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
RedHat RHSA: RHSA-2008:0008
Secunia Advisory ID: 28526, 28749, 28977, 29348, 29420, 29640, 30621, 31026, 31404, 31416, 31651, 31904, 32222, 32575, 32685, 32838, 33156, 33797, 34219, 34259, 34418
Security Tracker: 1020267
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html

Issue Description:

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9.
There are a number of vulnerabilities that affect version prior to 2.2.9.

Such versions may be affected by several issues, including:;;
- Improper handling of excessive forwarded interim responses may cause denial-of-service conditions in mod_proxy_http (CVE-2008-2364).
- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer (CVE-2007-6420).;
- Apache htpasswd Password Entropy Weakness;
- Apache 'mod_negotiation' HTML Injection and HTTP Response Splitting Vulnerability;
Note: that the remote web server may not actually be affected by these vulnerabilities.
HackRack/BroadView did not try to determine whether the affected modules are in use or to check for the issues themselves.

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

Apache < 2.2.8 Multiple Vulnerabilities

Impact: Level 4 - Critical

192.168.235.61 : Potential Vulnerabilities

CVSS Score: 7.8

CVE Reference: CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423, CVE-2007-6514, CVE-2008-0005, CVE-2008-0455, CVE-2008-0456, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 31118
Bugtraq ID: 26663, 26838, 27234, 27236, 27237, 27409, 8707
CVE ID: 2007-6203, 2007-5000, 2007-6388, 2008-0005, 2007-6420,2007-6421, 2007-6422, 2007-6423
FrSIRT Advisory: ADV-2007-4060, ADV-2007-4201, ADV-2007-4202, ADV-2007-4301, ADV-2008-0047, ADV-2008-0048
ISS X-Force ID: 38800, 39002, 39001, 39615
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0135.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0193.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-03/0159.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-11/0150.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Other Advisory URL: HPSBUX02308 SSRT080010
Other Advisory URL: HPSBUX02313 SSRT080015
Other Advisory URL: HPSBUX02431 SSRT090085
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2008-July/000370.html
Other Advisory URL: http://procheckup.com/Vulnerability_PR07-37.php
Other Advisory URL: http://securityreason.com/achievement_securityalert/49
Other Advisory URL: http://securityreason.com/securityalert/3523
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-233623-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK62966
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200801e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200807e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200808e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200803-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:014

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:015
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
Other Advisory URL:
https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/install/v61.Readme.html#MH01110
RedHat RHSA: RHSA-2008:0004, RHSA-2008:0005, RHSA-2008:0006, RHSA-2008:0007, RHSA-2008:0008
Secunia Advisory ID: 27906, 28046, 28073, 28081, 28082, 28196, 28375, 28467, 28471, 28525, 28526, 28607, 28749, 28750, 28922, 28965, 28977, 29348, 29420, 29504, 29640, 29806, 29988, 30356, 30430, 30732, 31026, 31142, 32222, 32575, 32800, 33105, 33200, 33797, 34219, 34219, 35650
Security Tracker: 1019030, 1019093, 1019154, 1019185
Snort Signature ID: 13302
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1897
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-042_e/index-e.html
Vendor Specific Advisory URL: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01756421
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_20.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58074
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg24019245
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: ftp://ftp.software.ibm.com/software/websphere/ihs/support/fixes/PK65782/

Issue Description:

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8.

Such versions may be affected by several issues, including:
- A cross-site scripting issue involving mod_imagemap (CVE-2007-5000).
- A cross-site scripting issue involving 413 error pages via a malformed HTTP method (PR 44014 / CVE-2007-6203).
- A cross-site scripting issue in mod_status involving the refresh parameter (CVE-2007-6388).
- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).
- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi-Processing Module is used (CVE-2007-6422).
- A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset (CVE-2008-0005).
- Apache 'mod_negotiation' HTML Injection and HTTP Response Splitting Vulnerability (CVE-2008-0455, CVE-2008-0456)
Note: that the remote web server may not actually be affected by these vulnerabilities. HackRack did not try to determine whether the affected modules are in use or to check for the issues themselves.

192.168.235.61 : Potential Vulnerabilities

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

Apache 2.2 < 2.2.14 Multiple Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.5

CVE Reference: CVE-2009-2699, CVE-2009-3094, CVE-2009-3095

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 42052
http://www.securityfocus.com/advisories/17947
http://www.securityfocus.com/advisories/17959
http://www.intevydis.com/blog/?p=59
https://issues.apache.org/bugzilla/show_bug.cgi?id=47645
http://www.apache.org/dist/httpd/CHANGES_2.2.14
BID:36254
OSVDB:57851, OSVDB:58879, Secunia:36549

Issue Description:

The remote web server is affected by multiple vulnerabilities.

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14.
Such versions are potentially affected by multiple vulnerabilities :
- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)
- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions.
(CVE-2009-3095)
- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp'module allows
remote FTP servers to cause a denial-of-service. (CVE-2009-3094)
Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not
try to determine whether the affected modules are in use or check for the issues themselves.

Suggestions:

Either ensure the affected modules are not in use or upgrade to Apache
version 2.2.14 or later.

Apache < 2.2.6 Multiple Vulnerabilities

192.168.235.61 : Potential Vulnerabilities

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2006-4110, CVE-2006-4154, CVE-2006-5752, CVE-2007-1741, CVE-2007-1742, CVE-2007-1743, CVE-2007-1862, CVE-2007-1863, CVE-2007-3303, CVE-2007-3304, CVE-2007-3847, CVE-2007-4465, CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423, CVE-2008-0455, CVE-2008-2168, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2008-1678

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 26023
Bugtraq ID: 24215, 24553, 24645, 24649, 25489, 25653, 21865, 25653
CVE ID: 2007-3303, 2007-3847, 2006-5752, 2007-4465, 2007-1862, 2007-3304
FrSIRT Advisory: ADV-2007-2727, ADV-2007-3100, ADV-2007-3020, ADV-2007-3095, ADV-2007-3283, ADV-2007-3494, ADV-2007-2231
ISS X-Force ID: 36586
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-05/0415.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-06/0251.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0129.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0102.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0184.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://mail-archives.apache.org/mod_mbox/httpd-dev/200706.mbox/%3c20070629141032.GA15192@redhat.com%3e
Mail List Post: http://marc.info/?l=apache-cvs&m=118592992309395&w=2
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118252946632447&w=2
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118595556504202&w=2
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=118595953217856&w=2
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc
Other Advisory URL: HPSBUX02262 SSRT071447
Other Advisory URL: HPSBUX02273 SSRT071476
Other Advisory URL: HPSBUX02365 SSRT080118
Other Advisory URL: HPSBUX02431 SSRT090085
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:140
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:141
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:142
Other Advisory URL: http://httpd.apache.org/security/vulnerabilities_20.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-11/msg00002.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-June/000207.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-September/000241.html
Other Advisory URL: http://security.psnc.pl/files/apache_report.pdf
Other Advisory URL: http://securityreason.com/achievement_securityalert/46
Other Advisory URL: http://securityreason.com/securityalert/2814

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: http://securityreason.com/securityalert/3113
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-103179-1
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-200032-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-351.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-363.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-500.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK49295
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK50467
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK50469
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702
Other Advisory URL: http://www-1.ibm.com/support/search.wss?rs=0&q=PK50467&apar=only
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200807e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:235
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2007:140
Other Advisory URL: http://www.redhat.com/errata/RHSA-2007-0532.html
Other Advisory URL: http://www.redhat.com/support/errata/RHSA-2007-0557.html
Other Advisory URL: http://www.redhat.com/support/errata/RHSA-2007-0662.html
Other Advisory URL: http://www.trustix.org/errata/2007/0026/
Other Advisory URL: http://www.ubuntu.com/usn/usn-499-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2007-September/msg00353.html
RedHat RHSA: RHSA-2007:0532, RHSA-2007:0556, RHSA-2007:0557, RHSA-2007:0662, RHSA-2007:0746, RHSA-2007:0534, RHSA-2007:0533, RHSA-2007:0911
Related OSVDB ID: 38939, 37050
Secunia Advisory ID: 26273, 25920, 25827, 25830, 26211, 26443, 26508, 26611, 26759, 26790, 26822, 27209, 27563, 27732, 26636, 26722, 26952, 26842, 27593, 27882, 27971, 28467, 28606, 28749, 28922, 26993, 29420, 30430, 25873, 27037, 26458, 28224, 28471, 28082, 28607, 31651, 33105, 35650
Security Tracker: 1018304, 1018633, 1018302
Snort Signature ID: 13309, 13310, 13311
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1897
Vendor Specific Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-041_e/index-e.html
Vendor Specific Advisory URL: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01756421
Vendor Specific News/Changelog Entry: http://bugs.gentoo.org/show_bug.cgi?id=186219
Vendor Specific News/Changelog Entry: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=245111
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_20.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry: http://issues.apache.org/bugzilla/show_bug.cgi?id=41551

192.168.235.61 : Potential Vulnerabilities

Vendor Specific News/Changelog Entry: http://issues.apache.org/bugzilla/show_bug.cgi?id=41551>
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=547987
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=549159
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27006876
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/CHANGES_2.2.6
Vendor Specific News/Changelog Entry: http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1500
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc

Issue Description:

According to its banner, the version of Apache installed on the remote host is older than 2.2.6. Such versions may be affected by several issues.

These issues include :
- A denial of service vulnerability in mod_proxy.
- A cross-site scripting vulnerability in mod_status.
- A local denial of service vulnerability associated with the Prefork MPM module.
- An information leak in mod_cache.
- A denial of service vulnerability in mod_cache.

In addition, it offers a workaround for a cross-site scripting issue in mod_autoindex.
Note: the remote web server may not actually be affected by these vulnerabilities. The scanner did not try to determine whether any of the affected modules are in use on the remote server or to check for the issues themselves.

Suggestions:

Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.6 or later.

Apache < 2.2.3

Impact: Level 4 - Critical

CVSS Score: 7.8

CVE Reference: CVE-2006-3747, CVE-2006-3918, CVE-2006-4110, CVE-2006-4154, CVE-2006-5752, CVE-2007-4465, CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423, CVE-2008-0455, CVE-2008-2168, CVE-2008-2939, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 31659

192.168.235.61 : Potential Vulnerabilities

Bugtraq ID: 19204, 19661, 19447, 20527, 24645, 25653, 26663, 26838, 27237, 27236, 27409, 29112, 30560
CERT VU: 395412, 663763
FrSIRT Advisory: ADV-2006-2963, ADV-2006-2964, ADV-2006-3264, ADV-2006-4207, ADV-2006-5089, ADV-2006-3265, ADV-2006-4033, ADV-2007-2727, ADV-2007-4060, ADV-2007-4201, ADV-2007-4202, ADV-2007-4301, ADV-2008-0047, ADV-2008-0048, ADV-2008-2315, ADV-2008-2461
Generic Exploit URL: http://downloads.securityfocus.com/vulnerabilities/exploits/apache-aug9-2006.html
Generic Exploit URL: http://www.metasploit.com
ISS X-Force ID: 29550, 36586, 38800, 39002, 39001, 39867, 42303, 44223
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-05/0151.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-05/0441.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-07/0425.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-07/0456.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-07/0514.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-08/0206.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-08/0398.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-10/0225.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2006-12/0089.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-08/0069.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-09/0129.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2007-10/0102.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-01/0332.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0018.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-02/0193.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-03/0159.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0131.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0137.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-06/0080.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0051.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-11/0150.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2006-07/0674.html
Mail List Post: http://archives.neohapsis.com/archives/fulldisclosure/2006-11/0102.html
Mail List Post: http://attrition.org/pipermail/vim/2006-November/001125.html
Mail List Post: http://attrition.org/pipermail/vim/2006-November/001126.html
Mail List Post: http://attrition.org/pipermail/vim/2007-November/001847.html
Mail List Post: http://attrition.org/pipermail/vim/2007-November/001849.html
Mail List Post: http://attrition.org/pipermail/vim/2007-November/001850.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=124621326524824&w=2
Mail List Post: http://marc.info/?l=apache-httpd-dev&m=124661528519546&w=2
Mail List Post: http://marc.info/?l=bugtraq&m=123376588623823&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/495180/100/0/threaded
Milw0rm: 2237
Other Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc
Other Advisory URL: HPSBUX02262 SSRT071447:
Other Advisory URL: HPSBUX02308 SSRT080010:

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: HPSBUX02313 SSRT080015:
Other Advisory URL: HPSBUX02365 SSRT080118:
Other Advisory URL: HPSBUX02431 SSRT090085:
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:140
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:141
Other Advisory URL: http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:142
Other Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01118771
Other Advisory URL: http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=421
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2007-11/msg00002.html
Other Advisory URL: http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2007-June/000207.html
Other Advisory URL: http://lists.rpath.com/pipermail/security-announce/2008-July/000370.html
Other Advisory URL: http://lists.suse.com/archive/suse-security-announce/2006-Sep/0004.html
Other Advisory URL: http://openbsd.org/errata.html#httpd2
Other Advisory URL: http://procheckup.com/Vulnerability_PR07-37.php
Other Advisory URL: http://securityreason.com/achievement_securityalert/46
Other Advisory URL: http://securityreason.com/securityalert/1294
Other Advisory URL: http://securityreason.com/securityalert/3113
Other Advisory URL: http://securityreason.com/securityalert/3523
Other Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-103179-1
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-200032-1
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-233623-1
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2007-351.htm
Other Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK24631
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK49295
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK62966
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg24013080
Other Advisory URL: http://www.apache.org/dist/httpd/Announcement1.3.html
Other Advisory URL: http://www.debian.org/security/2006/dsa-1167
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200801e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200802e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200807e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200808e.html
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200809e.html

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200608-01.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200610-12.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200711-06.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200803-19.xml
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:235
Other Advisory URL: http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:016
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2009:149
Other Advisory URL: http://www.mindedsecurity.com/MSA01150108.html
Other Advisory URL: http://www.niscc.gov.uk/niscc/docs/al-20060728-00515.html?lang=en
Other Advisory URL: http://www.novell.com/linux/security/advisories/2006_51_apache.html
Other Advisory URL: http://www.rapid7.com/advisories/R7-0033
Other Advisory URL: http://www.secuobs.com/secumail/snsecumail/msg01982.shtml
Other Advisory URL: http://www.trustix.org/errata/2007/0026/
Other Advisory URL: http://www.ubuntu.com/usn/usn-499-1
Other Advisory URL: http://www.ubuntu.com/usn/usn-575-1
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1131
Other Advisory URL: http://www.us.debian.org/security/2006/dsa-1132
Other Advisory URL: https://bugzilla.redhat.com/show_bug.cgi?id=489436
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
Other Advisory URL:
https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/install/v61.Readme.html#MH01110
RedHat RHSA: https://rhn.redhat.com/errata/RHSA-2009-1148.html
RedHat RHSA: RHSA-2006:0618, RHSA-2006:0692, RHSA-2006:0619, RHSA-2007:0556, RHSA-2007:0532, RHSA-2007:0534, RHSA-2007:0533, RHSA-2007:0557, RHSA-2007:0911, RHSA-2008:0004, RHSA-2008:0005, RHSA-2008:0006, RHSA-2008:0007, RHSA-2008:0008, RHSA-2008:0967, RHSA-2008:0966, RHSA-2009:1075
Related OSVDB ID: 47474
Secunia Advisory ID: 21172, 21174, 21197, 21241, 21245, 21247, 21266, 21273, 21284, 21307, 21313, 21315, 21346, 21399, 21478, 21490, 21509, 21598, 21744, 21848, 21986, 22140, 22262, 22317, 22368, 22388, 22458, 22523, 22549, 22669, 23260, 25827, 25830, 25873, 25920, 26211, 26273, 26329, 26443, 26458, 26508, 26822, 26842, 26952, 26993, 27037, 27563, 27732, 27882, 27906, 28046, 28073, 28081, 28082, 28196, 28224, 28375, 28467, 28471, 28525, 28526, 28606, 28607, 28749, 28750, 28922, 28965, 28977, 29348, 29420, 29504, 29640, 29806, 29849, 29988, 30356, 30430, 30732, 31026, 31142, 31384, 31651, 31673, 32222, 32575, 32685, 32800, 32838, 33105, 33156, 33200, 33428, 33797, 33933, 34219, 35074, 35261, 35264, 35395, 35453, 35650, 35691, 35721, 35781, 35793, 35813, 35823, 35865, 35871, 1016569
Security Tracker: 1016569, 1018302, 1019030, 1019093, 1019154 ,1019256, 1020635
Snort Signature ID: 11679, 13302
Vendor Specific Advisory URL: ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P.asc
Vendor Specific Advisory URL: http://docs.info.apple.com/article.html?artnum=307562
Vendor Specific Advisory URL:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE
Vendor Specific Advisory URL: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific Advisory URL: http://itrc.hp.com/service/cki/docDisplay.do?docId=c00797078
Vendor Specific Advisory URL: http://openbsd.org/errata.html#httpd2
Vendor Specific Advisory URL: http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.610131

192.168.235.61 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102662-1
Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102663-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1222
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1897
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific Advisory URL: http://support.avaya.com/elmodocs2/security/ASA-2006-194.htm
Vendor Specific Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK24631
Vendor Specific Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK29154
Vendor Specific Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK29156
Vendor Specific Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg24013080
Vendor Specific Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f
/interstage-200802e.html
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200907-04.xml
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-041_e/index-e.html
Vendor Specific Advisory URL: http://www.hitachi-support.com/security_e/vuls_e/HS07-042_e/index-e.html
Vendor Specific Advisory URL: http://www.mandriva.com/security/advisories?name=MDKSA-2006:133
Vendor Specific Advisory URL: http://www.novell.com/linux/security/advisories/2006_43_apache.html
Vendor Specific Advisory URL: http://www.openbsd.org/errata.html#httpd
Vendor Specific Advisory URL: http://www.trustix.org/errata/2006/0044/
Vendor Specific Advisory URL: http://www.ubuntu.com/usn/usn-328-1
Vendor Specific Advisory URL: http://www.us.debian.org/security/2006/dsa-1167
Vendor Specific Advisory URL: http://www12.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01428449
Vendor Specific Advisory URL: http://www13.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01756421
Vendor Specific Advisory URL: https://issues.rpath.com/browse/RPL-538
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=534712
Vendor Specific News/Changelog Entry: http://bugs.gentoo.org/show_bug.cgi?id=186219
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_13.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_20.html
Vendor Specific News/Changelog Entry: http://httpd.apache.org/security/vulnerabilities_22.html
Vendor Specific News/Changelog Entry:
http://kb.vmware.com/KanisaPlatform/Publishing/466/5915871_f.SAL_Public.html
Vendor Specific News/Changelog Entry: http://lists.debian.org/debian-security-announce/2009/msg00128.html
Vendor Specific News/Changelog Entry: http://lists.debian.org/debian-security-announce/2009/msg00148.html
Vendor Specific News/Changelog Entry: http://support.avaya.com/elmodocs2/security/ASA-2006-194.htm
Vendor Specific News/Changelog Entry:
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587
Vendor Specific News/Changelog Entry:
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?revision=790587
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_pr
oxy_http.c?r1=790587&r2=790586&pathrev=790587
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=394965
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682868
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682870
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682871
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=790587
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=394965
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=549159
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=772997
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024

192.168.235.61 : Potential Vulnerabilities

Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg1PK58074
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg24019245
Vendor Specific News/Changelog Entry: http://www-1.ibm.com/support/docview.wss?uid=swg27007951
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/Announcement1.3.html
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/Announcement2.0.html
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/Announcement2.2.html
Vendor Specific News/Changelog Entry: http://www.apache.org/dist/httpd/CHANGES_2.2.6
Vendor Specific News/Changelog Entry: http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00320.html
Vendor Specific News/Changelog Entry: http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
Vendor Specific News/Changelog Entry: http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
Vendor Specific News/Changelog Entry: https://bugzilla.redhat.com/show_bug.cgi?id=509125
Vendor Specific News/Changelog Entry: https://issues.rpath.com/browse/RPL-1500
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-July/000931.html
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-June/000915.html
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: ftp://ftp.software.ibm.com/software/websphere/ihs/support/fixes/PK65782/
Vendor Specific Solution URL: ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
Vendor Specific Solution URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1
Vendor Specific Solution URL: http://svn.apache.org/viewvc?view=rev&revision=791454
Vendor URL: http://httpd.apache.org/
Vendor URL: http://tcl.apache.org/
Vendor URL: http://www.apache.org/

Issue Description:

The remote host appears to be running a version of Apache which is older than 2.2.3.

This version is vulnerable to an off-by-one buffer overflow attack in the mod_rewrite module.

Suggestions:

Upgrade to the latest version of Apache. Please see: http://httpd.apache.org

Apache HTTP Server OS Fingerprinting Unspecified Security Vulnerability

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

192.168.235.61 : Potential Vulnerabilities

Other References:

Nessus NASL ID : 95173

Issue Description:

Apache is prone to an unspecified security vulnerability related to OS fingerprinting at the application-level.
Affected Products:
Apache 2.2.9 and prior

Very few details are available regarding this issue. We will update this plugin when more information becomes available.

Suggestions:

Upgrade to the latest version of Apache 2.2, which is available for download from the Apache Web site.

Apache 2.x < 2.2.12 Multiple Vulnerabilities

Impact: Level 3 - High

CVE Reference: CVE-2008-2939, CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 40467
Bugtraq ID: 30560, 34663, 35221, 35253
CERT VU: 663763
CVE ID: 2008-2939, 2009-1191, 2009-1195, 2009-0023, 2009-1955, 2009-1956, 2009-1890, 2009-1891

Issue Description:

The remote web server may be affected by several issues.

According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12.
Such versions may be affected by several issues, including :
- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)
- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body.

192.168.235.61 : Potential Vulnerabilities

(CVE-2009-1191)
- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)
- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy
configuration. (CVE-2009-1890)
- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)
- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)
- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)
Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Suggestions:

Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

Apache 2.2 < 2.2.11

Impact: Level 3 - High

CVSS Score: 5

CVE Reference: CVE-2008-2939, CVE-2008-2364, CVE-2009-1191

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95123
Bugtraq ID: 29653, 30560, 34663
CERT VU: 663763
CVE ID: 2008-2364, 2008-2939, 2009-1191
FrSIRT Advisory: ADV-2008-1798, ADV-2008-2315, ADV-2008-2461
ISS X-Force ID: 42987, 44223, 50059
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0051.html

192.168.235.61 : Potential Vulnerabilities

Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0261.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Mail List Post: http://marc.info/?l=bugtraq&m=123376588623823&w=2
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/495180/100/0/threaded
Other Advisory URL: HPSBUX02365 SSRT080118:
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg27008517
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200809e.html
Other Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200807-06.xml
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:195
Other Advisory URL: http://www.rapid7.com/advisories/R7-0033
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00055.html
Other Advisory URL: https://www.redhat.com/archives/fedora-package-announce/2008-August/msg00153.html
RedHat RHSA: RHSA-2008:0966, RHSA-2008:0967
Related OSVDB ID: 47474
Secunia Advisory ID: 30621, 31026, 31384, 31404, 31416, 31651, 31673, 31904, 32222, 32575, 32685, 32838, 33156, 33428, 33797, 33933, 34219, 34259, 34418, 34827, 35074, 35395, 35721
Security Tracker: 1020267
Security Tracker: 1020635
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1222
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3216
Vendor Specific Advisory URL: http://www.gentoo.org/security/en/glsa/glsa-200907-04.xml
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00001.html
Vendor Specific News/Changelog Entry: http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00004.html
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=666154&r2=666153&pathrev=666154
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682868
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682870
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682871
Vendor Specific News/Changelog Entry: https://issues.apache.org/bugzilla/show_bug.cgi?id=46949
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-June/000915.html
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1

192.168.235.61 : Potential Vulnerabilities

Vendor Specific Solution URL: http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Issue Description:

Apache 2.2 version is older than 2.2.11.

According to the version number of the Apache banner on the remote host, the Apache 2.2 version may be vulnerable to a number of flaws, some of which allow code execution.
These include the following:
CVE-2008-2939 - Apache mod_proxy_ftp Directory Component Wildcard Character XSS
CVE-2008-2364 - Apache mod_proxy ap_proxy_http_process_response() Function Interim Response Forwarding Remote DoS
CVE-2009-1191 - Apache mod_proxy_ajp Cross Thread/Session Information Disclosure

Suggestions:

Upgrade to the latest version of Apache 2.2. Please see: http://httpd.apache.org

OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056)

Impact: Level 3 - High

CVSS Score: 4.6

CVE Reference: CVE-2006-0225

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95233
BugTraq ID: 16369
http://www.openssh.com/
http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00062.html
http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
http://www.vmware.com/support/vi3/doc/esx-3069097-patch.html

Issue Description:

OpenSSH is a freely available, open source implementation of the Secure Shell protocol. It is available for multiple platforms, including Unix, Linux and Microsoft. SCP is a secure copy application that is a part of OpenSSH. It is used to copy files from one computer to another over an SSH connection. If SCP is given all-local paths to copy, it acts like the system "cp" command.
OpenSSH is susceptible to a local SCP shell command execution vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input prior to utilizing it in a "system()" function call.

192.168.235.61 : Potential Vulnerabilities

If SCP is used in an all-local fashion, without any hostnames, it utilizes the "system()" function to execute a local copy operation. By utilizing the "system()" function, a shell is spawned to process the arguments. If filenames are created that contain shell metacharacters, they will be processed by the shell during the "system()" function call. Attackers can create files with names that contain shell metacharacters along with commands to be executed. If a local user then utilizes SCP to copy these files (likely during bulk copy operations involving wildcards), then the attacker-supplied commands will be executed with the privileges of the user running SCP.
This issue reportedly affects OpenSSH Version 4.2. Other versions may also be affected.

This issue can allow local attackers to execute arbitrary shell commands with the privileges of users executing a vulnerable version of SCP.

Suggestions:

If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056.
HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details.
Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates.
You can confirm if this vulnerability is present on your computer as follows.
On a Unix prompt, type these commands:
a. touch foo bar
b. mkdir "any_directory"
c. scp foo bar "any_directory"
If the output is:
"cp: cannot stat `foo': No such file or directory
cp: cannot stat `bar': No such file or directory"
then your OpenSSH is vulnerable. Refer to the following link for Redhat advisoryRHSA-2006:0044-14.
Refer to Vmware advisoryVMware Patch 9986131,
yVMware Patch 3069097.

OpenSSH X11 Session Hijacking Vulnerability

Impact: Level 3 - High

CVE Reference: CVE-2008-1483

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 31737
Bugtraq ID: 28444
Secunia Advisory ID 229522, 29537, 29554, 29626, 29627, 29676, 29683, 29686, 29721, 29735, 29873, 29939, 30086, 30230, 30249, 30347, 30361, 31531, 31882
Vendor Specific Advisory URL:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01462841

192.168.235.61 : Potential Vulnerabilities

Vendor Specific Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-237444-1
Vendor Specific Advisory URL: http://support.apple.com/kb/HT3137
Vendor Specific News/Changelog Entry: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
Vendor Specific News/Changelog Entry: http://sourceforge.net/project/shownotes.php?release_id=590180

Issue Description:

According to its banner, the version of SSH installed on the remote host is older than 5.0.

Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

Suggestions:

Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org

Apache mod_proxy_ftp Globbing Cross-Site Scripting Vulnerability

Impact: Level 3 - High

CVSS Score: 4.3

CVE Reference: CVE-2008-2939

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 34433
Bugtraq ID: 30560
CERT VU: 663763
CVE ID: 2008-2939
FrSIRT Advisory: ADV-2008-2315, ADV-2008-2461
ISS X-Force ID: 44223
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2008-08/0051.html
Mail List Post: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00000.html
Mail List Post: http://archives.neohapsis.com/archives/bugtraq/2009-03/0009.html
Mail List Post: http://www.securityfocus.com/archive/1/archive/1/495180/100/0/threaded
Mail List Post: http://marc.info/?l=bugtraq&m=123376588623823&w=2
Other Advisory URL: http://www.rapid7.com/advisories/R7-0033
Other Advisory URL: http://www-01.ibm.com/support/docview.wss?uid=swg1PK70937
Other Advisory URL: http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0328
Other Advisory URL: http://sunsolve.sun.com/search/document.do?assetkey=1-66-247666-1
Other Advisory URL: http://www.fujitsu.com/global/support/software/security/products-f/interstage-200809e.html
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70197
Other Advisory URL: http://www-1.ibm.com/support/docview.wss?uid=swg1PK70937

192.168.235.61 : Potential Vulnerabilities

Other Advisory URL: http://www.mandriva.com/security/advisories?name=MDVSA-2008:194
Other Advisory URLh: ttp://www.mandriva.com/security/advisories?name=MDVSA-2008:195
RedHat RHSA: RHSA-2008:0967, RHSA-2008:0966
Related OSVDB ID: 47474
Secunia Advisory ID: 31384, 31673, 32575, 32685, 32838, 33156, 33428, 33797, 34219, 35074, 33933
Security Tracker: 1020635
Vendor Specific Advisory URL: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01650939
Vendor Specific Advisory URL: http://support.apple.com/kb/HT1222
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682868
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682871
Vendor Specific News/Changelog Entry: http://svn.apache.org/viewvc?view=rev&revision=682870
Vendor Specific News/Changelog Entry: https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-March/000856.html
Vendor Specific Solution URL: http://sunsolve.sun.com/search/document.do?assetkey=1-26-247666-1

Issue Description:

The mod_proxy_ftp module in the version of Apache installed on the remote host fails to properly sanitize user-supplied URL input before using it to generate dynamic HTML output.

Using specially crafted requests for FTP URLs with globbing characters (such as asterisk, tilde, opening square bracket, etc), an attacker may be able to leverage this issue to inject arbitrary HTML and script code into a user's browser to be executed within the security context of the affected site.

Suggestions:

Either disable the affected module or upgrade to Apache version 2.2.10 or later.

Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day

Impact: Level 3 - High

CVE Reference: No CVE Reference At This Time

Port/Protocol: 80/TCP

Other References:

Nessus NASL ID : 95219

Issue Description:

The Apache HTTP Server, commonly referred to as Apache is a freely available Web server.
Apache is vulnerable to a denial of service due to holding a connection open for partial HTTP requests.
Apache Versions 1.x and 2.x are vulnerable.

192.168.235.61 : Potential Vulnerabilities

A remote attacker can cause a denial of service against the Web server which would prevent legitimate users from accessing the site.
Denial of service tools and scripts such as Slowloris takes advantage of this vulnerability.

Suggestions:

Patch:
There are no vendor-supplied patches available at this time.
Workaround:
-Reverse proxies, load balancers and iptables can help to prevent this attack from occurring.
-Adjusting the TimeOut Directive can also prevent this attack from occurring.

OpenSSH GSSAPI Credential Disclosure Vulnerability

Impact: Level 2 - Medium

CVSS Score: 5

CVE Reference: CVE-2005-2798

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 19592
http://www.mindrot.org/pipermail/openssh-unix-announce/2005-September/000083.html

Issue Description:

According to its banner, the version of OpenSSH installed on the remote host may allow GSSAPI credentials to be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled.

Suggestions:

Upgrade to OpenSSH 4.2 or later.

OpenSSH < 5.2/5.2p1

Impact: Level 2 - Medium

CVSS Score: 1.2

192.168.235.61 : Potential Vulnerabilities

CVE Reference: CVE-2008-3259

Port/Protocol: 22/TCP

Other References:

Nessus NASL ID : 95122
Bugtraq ID: 30339
CVE ID: 2008-3259
FrSIRT Advisory: ADV-2008-2148
ISS X-Force ID: 43940
Secunia Advisory ID: 31179
Security Tracker: 1020537
Vendor Specific News/Changelog Entry: http://openssh.com/security.html
Vendor Specific News/Changelog Entry: http://www.openssh.com/txt/release-5.1

Issue Description:

OpenSSH version is older than 5.2/5.2p1.

According to the version number of the OpenSSH daemon (opensshd) on the remote host, the OpenSSH version may be vulnerable to a number of flaws.
A list of the possible vulnerabilities, related with versions < 5.2, is below:
CVE-2008-3259 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Suggestions:

Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
SNMP Weak / Guessable Community String SNMP should preferably be removed if not in use.;; Alternatively, the following security precautions should be put in place:; - All community strings should be set to stronger, less easily guessable alternatives.; - If SNMP is only used for monitoring purposes, write access should be disabled.; - SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).; - Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;; For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:; Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;		☐
Writeable SNMP Information If SNMP access is not required on this system, then disallow it. Otherwise, use a secure un-guessable "community name", and restrict the hosts that talk SNMP with your system to a defined list of IP addresses.		☐
		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
Cisco Default Password Access this device and set a password using 'enable secret'		
Cisco Multiple Devices Crafted IP Option Multiple Remote Code Execution Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb157.shtml		☐
Cisco IOS System Timers Remote Overflow (CSCei61732) Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml		☐
SSH Weak Cipher Used Where possible SSH should be configured not to use weak ciphers such as DES. A more secure alternative is available in most cases e.g. 3DES, AES.		☐
Outdated SSH Protocol Versions Supported If you use OpenSSH, set the option 'Protocol' to '2'. If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.		☐
		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
Cisco IOS SAA Malformed RTR Packet DoS (CSCdx17916, CSCdx61997) Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml		
Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-ud) Workarounds: 1) Disable affected listening ports. Once disabled, confirm that the listening UDP port has been closed by entering the CLI command "show udp" or "show ip socket". Impact of workaround #1: When applying this workaround to devices that are processing MGCP or H.323 calls, the device will not allow stopping SIP processing while active calls are being processed. 2) Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks. 3) Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Impact of workaround #2 and #3: Because the features in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. 4) Use Cisco IOS Embedded Event Manager (EEM) policy to detect blocked interface queues. EEM can alert administrators of blocked interfaces with email, a syslog		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
message, or a Simple Network Management Protocol (SNMP) trap. Further information and examples on mitigating the vulnerability through workarounds can be found at the advisory cisco-sa-20090325-udp. Patch: Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-udp for additional information on obtaining the fixes.		
Cisco IOS SSL Packets Multiple Vulnerabilities Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20070522-SSL for further information.		☐
Cisco IOS Next Hop Resolution Protocol Vulnerability Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco security advisory cisco-sa-20070808 for further information.		☐
Cisco IOS TCP Listener Crafted Packets Remote DoS Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml		☐
Cisco IOS Multiple DLSw Denial of		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
Service Vulnerabilities Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080326-dlsw for information.		
Cisco Telnet Denial of Service Vulnerability Solution : http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed. These worarounds are: - Enabling SSH and disabling telnet - Configuring a VTY Access Class - Configuring Access Lists (ACLs) - Configuring Infrastructure Access Lists (iACLs) - Configuring Receive Access Lists (rACLs) - Clearing Hung TCP Connections Using the IOS CLI - Clearing Hung TCP Connections Using SNMP		☐
Cisco IOS ICMP Redirect Routing Table Modification Workaround: The following workaround was suggested. It is possible to prevent the router from acting upon ICMP redirect packets by issuing		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
the following command on the affected device: Router(config)#no ip icmp redirect Solution: Users are advised to upgrade to the following IOS versions: 12.2(13.03)B 12.2(12.05)T 12.2(12.05)S 12.2(12.05) 12.2(12.02)S 12.2(12.02)T		
Cisco IOS EIGRP Announcement ARP Denial of Service Vulnerability The workaround for this issue is to apply MD5 authentication that will permit the receipt of EIGRP packets only from authorized hosts. You can find an example of how to configure MD5 authentication for EIGRP here. If you are using EIGRP in the unicast mode then you can mitigate this issue by placing appropriate ACL which will block all EIGRP packets from illegitimate hosts.		☐
Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip) 1) For devices that do not require SIP to be enabled, the simplest and most effective workaround is to disable SIP processing on the device. On some Cisco IOS software versions, SIP can be disabled using the following commands: sip-ua no transport udp no transport tcp Impact of the workaround: When applying this workaround to devices		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
that are processing Media Gateway Control Protocol (MGCP) or H.323 calls, the device will not stop SIP processing while active calls are being processed. 2) For devices that need to offer SIP services it is possible to use Control Plane Policing (CoPP) to block SIP traffic to the device from untrusted sources. Impact of the workaround: Because SIP can use UDP as a transport protocol, it is possible to easily spoof the IP address of the sender, which may defeat access control lists that permit communication to these ports from trusted IP addresses. Further information and examples on disabling SIP and configuring CoPP to block SIP traffic can be found at the advisory cisco-sa-20090325-sip. Patch: Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-sip for additional information on obtaining the fixes.		
Cisco IOS Software Multiple Multicast Vulnerabilities (cisco-sa-20080924-multicast) Cisco released an advisory detailing various workarounds and solutions. Refer to Cisco Security Advisory cisco-sa-20080924-ubr for more information.		☐
Cisco IOS Interface DoS Cisco has released updated IOS		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml		
Cisco IOS and Unified Communications Manager Multiple Voice Vulnerabilities Cisco released an advisory detailing various workarounds and solutions. Refer to the following Cisco Security Advisory: Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager (Document ID 98182).		☐
Cisco IOS Secure Shell Server TACACS+ Multiple DoS (CSCed65778, CSCed65285) Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml		☐
Vulnerabilities in the Internet Key Exchange Xauth Implementation Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml		☐
Cisco Malformed SNMP Message Handling DoS (CSCdw67458) Cisco has released updated IOS software to fix this vulnerability.		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
Also, as list of potential workarounds http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml		
Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip) - Use Infrastructure Access Control Lists (iACLs) to block traffic at the border of networks. - Use Receive ACL (rACL) to protect the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. - Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Further information and examples on configuring iACLs, rACLs and CoPP can be found at the advisory cisco-sa-20090325-ip. Patch: Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco-sa-20090325-ip for additional information on obtaining the fixes.		☐
UDP Constant IP Identification Field Fingerprinting Vulnerability We are not currently aware of any fixes for this issue.		☐
Management Interfaces Accessible On Cisco Device Vulnerability Disable services that are not		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
needed. Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall. Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible. Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.		
Unencrypted Telnet Server Disable this service and use SSH instead.		☐
Management Interfaces Accessible On Cisco Device Vulnerability Disable services that are not needed. Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall. Use secure services like (HTTPS, SSH) instead of HTTP or TELNET if possible. Do not use default passwords and replace them with hard to guess passwords. Change passwords frequently.		☐
Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels) Solution: Cisco has released an advisory		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
detailing solutions available to fix the issue. Refer to Cisco Security Advisory cisco-sa-20090923-tunnels for additional information on obtaining the fixes. Workarounds: Disabling Cisco Express Forwarding will mitigate this vulnerability. It can be disabled in the following two ways: 1) Disable Cisco Express Forwarding Globally by using the no ip cef and no ipv6 cef global configuration commands. 2) Disable Cisco Express Forwarding on all Tunnel Interfaces configured on an affected device as shown in the following example: interface Tunnel [interface-ID] no ip route-cache cef Impact of the workaround: Disabling Cisco Express Forwarding may have significant performance impact and is not recommended by Cisco. Refer to the advisory for additional details on the workarounds.		
Cisco IOS NTP Daemon Buffer Overflow Vulnerability Customers with service contracts should obtain upgraded software through their regular update channels for any software release containing the feature sets they have purchased. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Web site.		☐
Cisco IOS Software TCP State Manipulation Denial of Service Vulnerabilities (cisco-sa-20090908-tcp24)		☐

192.168.235.49 : Recommendations

Recommendations	Comments	Completed
Patch: Cisco has released an advisory detailing various solutions available to fix this issue. Refer to Cisco Security Advisory cisco sa-20090908-tcp24 for additional information on obtaining the fixes. Workarounds: Cisco has guidelines for mitigation against the TCP state manipulation vulnerabilities for Cisco IOS Software, CatOS Software, ASA and PIX Software and Nexus Software. Please refer to Workaround Section at cisco-sa-20090908-tcp24 for detailed guidelines.		
Cisco IOS TCLSH AAA Command Authorization Bypass Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml		☐
Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability Cisco has released updated IOS software to fix this vulnerability. Also, as list of potential workarounds can be found at: http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
SSL 2.0 Protocol Usage Make sure to disable the SSL 2.0 protocol OpenSSL 0.9.7 branch: Update to version 0.9.7h or later. OpenSSL 0.9.8 branch: Update to version 0.9.8a or later. IIS: http://support.microsoft.com/kb/187498 or http://support.microsoft.com/kb/245030/		☐
SNMP Weak / Guessable Community String SNMP should preferably be removed if not in use.;; Alternatively, the following security precautions should be put in place:; - All community strings should be set to stronger, less easily guessable alternatives.; - If SNMP is only used for monitoring purposes, write access should be disabled.; - SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).; - Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;; For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:; Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
Service >> right click, select Properties >> Security.;		
OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org		☐
SSH version older than 3.4 Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org		☐
OpenSSH Buffer Management Vulnerability (OpenSSH < 3.7.1) This issue is resolved in OpenSSH releases 3.7.1 and later. Upgrade to latest stable release version of OpenSSH available from www.openssh.com. Manual patches for this issue are available from http://www.openssh.com/txt/buffer.adv. For vendor specific patch information, look up the vendor in question from http://www.securityfocus.com/bid/8628/solution, or contact the vendor directly.		☐
OpenSSH < 5.0 Upgrade to the latest version of OpenSSH. Please see: www.openssh.org		☐
OpenSSH < 4.0 Upgrade to the latest version of OpenSSH. Please see: www.openssh.org		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
Outdated SSH Protocol Versions Supported If you use OpenSSH, set the option 'Protocol' to '2'. If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.		☐
CGI Generic SQL Injection (blind) Modify the affected CGI scripts so that they properly escape arguments.		☐
IP Forwarding Enabled Disable IP fowarding by following the appropriate instructions below: On Windows 2000 and Windows NT, set the value of the following registry key to zero: HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParametersIPEnableRouter On Linux, insert this line in your startup script: "sysctl -w net.ipv4.ip_forward=0" On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup script: "ndd -set /dev/ip ip_forwarding 0" On Mac OS X, insert this line in your startup script: "sysctl -w net.inet.ip.forwarding=0"		☐
OpenSSH Reverse DNS Lookup bypass Upgrade to the latest stable release version of OpenSSH, available from http://www.openssh.org. This problem is resolved in OpenSSH 3.6.2 and later.		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
OpenSSH AFS/Kerberos ticket/token passing Upgrade to the latest version of OpenSSH. Please see: http://www.openssh.org		☐
Self-signed certificate Please install a server certificate signed by a trusted third-party Certificate Authority.		☐
SSL Certificate Signed using Weak Hashing Algorithm Contact the Certificate Authority to have the certificate reissued.		☐
Unencrypted Telnet Server Disable this service and use SSH instead.		☐
SSL Medium Strength Cipher Suites Supported Reconfigure the affected application if possible to avoid use of medium strength ciphers.		☐
AutoComplete Attribute Not Disabled for Password in Form Based Authentication Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
SSL Certificate - Signature Verification Failed Vulnerability Please install a server certificate signed by a trusted third-party Certificate Authority.		☐
Weak Supported SSL Ciphers Suites Reconfigure the affected application if possible to avoid use of weak ciphers.		☐
TCP Sequence Number Approximation Please see http://www.securityfocus .com/bid/10183/solution, for the right solution for your infrastructure.		☐
Expect Header Cross-Site Scripting Vulnerability Check with the vendor for an update to the web server. For Apache, the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2. For IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1. For IBM WebSphere Application Server, upgrade to 5.1.1.17.		☐
OpenSSH X11 Session Hijacking Vulnerability Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org		☐
Netscape/OpenSSL Cipher Forcing Bug This problem can be fixed by		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
disabling the SSL_OP_NETSCAPE_REUSE _CIPHER_CHANGE_BUG option from the options list of OpenSSL's libssl library. This can be done by replacing the SSL_OP_ALL definition in the openssl/ssl.h file with the following line: #define SSL_OP_ALL (0x00000FFFL^SSL _OP_NETSCAPE_REUSE_CIPHER_CHANGE_BU G) The library and all programs using this library need to be recompiled to ensure that the correct OpenSSL library is used during linking.		
OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056) If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056. HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details. Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates. You can confirm if this vulnerability is present on your computer as follows. On a Unix prompt, type these commands: a. touch foo bar b. mkdir "any_directory" c. scp foo bar "any_directory" If the output is: "cp: cannot stat `foo': No such file or directory cp: cannot stat `bar': No such file or directory" then your OpenSSH is vulnerable. Refer to the following link for Redhat advisoryRHSA-2006:0044-14.		☐

192.168.235.51 : Recommendations

Recommendations	Comments	Completed
Refer to Vmware advisoryVMware Patch 9986131, yVMware Patch 3069097.		

192.168.235.52 : Recommendations

Recommendations	Comments	Completed
SNMP Weak / Guessable Community String SNMP should preferably be removed if not in use.;; Alternatively, the following security precautions should be put in place:; - All community strings should be set to stronger, less easily guessable alternatives.; - If SNMP is only used for monitoring purposes, write access should be disabled.; - SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).; - Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;; For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:; Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;		☐
SSL 2.0 Protocol Usage Make sure to disable the SSL 2.0 protocol OpenSSL 0.9.7 branch: Update to version 0.9.7h or later. OpenSSL 0.9.8 branch: Update to version 0.9.8a or later. IIS: http://support.microsoft.com/kb/187498 or		☐

192.168.235.52 : Recommendations

Recommendations	Comments	Completed
http://support.microsoft.com/kb/245030/		
Writeable SNMP Information If SNMP access is not required on this system, then disallow it. Otherwise, use a secure un-guessable "community name", and restrict the hosts that talk SNMP with your system to a defined list of IP addresses.		☐
Multiple Vendor Malformed SNMP Trap Handling DoS See www.cert.org/advisories/CA-2002-03.html		☐
3Com Wireless Access Point Default Password Vulnerability Configure a user name and password that are difficult for a malicious user to guess.		☐
3Com Wireless Access Point Default Password Vulnerability Configure a user name and password that are difficult for a malicious user to guess.		☐
SSL Medium Strength Cipher Suites Supported Reconfigure the affected application if possible to avoid use of medium strength ciphers.		☐
Weak Supported SSL Ciphers Suites		☐

192.168.235.52 : Recommendations

Recommendations	Comments	Completed
Reconfigure the affected application if possible to avoid use of weak ciphers.		
Web Server Uses Plain Text Authentication Forms Ensure that all sensitive information is transmitted to the remote webserver securely. SSL is the most common means of providing this security.		☐
Unencrypted Telnet Server Disable this service and use SSH instead.		☐

192.168.235.54 : Recommendations

Recommendations	Comments	Completed
SMB Login To fix this issue, edit the following key : HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2. Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.		☐
Oracle Default Accounts Disable all the default accounts.		☐
Oracle Critical Patch Update - January 2009 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html		☐
Malicious Software: NetBus Pro This software should be removed immediately and is indicative of a possible compromise of the host. Best practice recommends that compromised hosts be rebuilt completely in case malware or rootkits have also been installed on the machine.		☐
Oracle Critical Patch Update - April 2008 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html		☐

192.168.235.54 : Recommendations

Recommendations	Comments	Completed
Oracle Critical Patch Update - October 2008 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html		☐
Oracle Critical Patch Update - April 2007 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html		☐
Oracle Critical Patch Update - January 2008 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html		☐
Oracle Critical Patch Update - April 2006 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2006.html		☐
Oracle Critical Patch Update - October 2006 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html		☐
Oracle Critical Patch Update - January 2007		☐

192.168.235.54 : Recommendations

Recommendations	Comments	Completed
Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html		
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008: http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx		☐
Oracle Critical Patch Update - July 2006 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html		☐
Oracle Critical Patch Update - January 2006 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html		☐
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644) Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx		☐
SMB NULL Session		☐

192.168.235.54 : Recommendations

Recommendations	Comments	Completed
Disable the use of SMB Null Sessions, should it not be a business requirement.		
Oracle Critical Patch Update - July 2008 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html		☐
Oracle Critical Patch Update - July 2007 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html		☐
SMB Browse List Enumeration Netbios ports should never be accesible from the Internet and should be blocked on the firewall.		☐
Business Document Files Available Verify that the information contained within the discovered Business document files do not contain information that should otherwise be restricted. Should files be found to contain information not suitable for public consumption it is recommended that these files be removed from anonymous viewing.		☐
Business Document Files Available Verify that the information contained within the discovered		☐

192.168.235.54 : Recommendations

Recommendations	Comments	Completed
Business document files do not contain information that should otherwise be restricted. Should files be found to contain information not suitable for public consumption it is recommended that these files be removed from anonymous viewing.		
Oracle Critical Patch Update - October 2007 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html		☐
Oracle Critical Patch Update - October 2005 Install the vendor supplied patch: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html		☐

192.168.235.55 : Recommendations

Recommendations	Comments	Completed
SMB Login To fix this issue, edit the following key : HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2. Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.		☐
MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008: http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx		☐
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644) Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx		☐
SMB NULL Session Disable the use of SMB Null Sessions, should it not be a business requirement.		☐
Disabled SMB Signing Workaround: Please refer to Microsoft's article		☐

192.168.235.55 : Recommendations

Recommendations	Comments	Completed
887429 for information on enabling SMB signing.		
Microsoft Windows Telnet Server Does Not Enforce NTLM Authentication Configure the service to accept NTLM authentication only for increased security during authentication. To learn how to configure Telnet NTLM Authentication, read Microsoft Knowledge Base article 201194.		☐
Unencrypted Telnet Server Disable this service and use SSH instead.		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
SMB Login To fix this issue, edit the following key : HKLMSystemCurrentControlSetControlLSARestrictAnonymous and set its value to 2. Under Windows XP, make sure that the keys RestrictAnonymousSam and RestrictAnonymous are both set to 1.		☐
SMB Local User Enumeration Informational plugin.		☐
Samba < 3.0.27 Multiple Vulnerabilities Upgrade to Samba version 3.0.27 or later. Please see: http://www.samba.org		☐
Samba < 3.0.25 Multiple Vulnerabilities Upgrade to Samba version 3.0.25 or later. Please see: http://www.samba.org		☐
Samba < 3.0.24 Multiple Flaws Upgrade to Samba 3.0.24 or newer. Please see: http://www.samba.org		☐
OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org		☐
		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
[DSA1222] DSA-1222-2 proftpd No suggestion at this time		
ProFTP Buffer Overflow Vulnerability Upgrade to ProFTPD version 1.3.0a or later. Please see: http://www.proftpd.org		☐
Samba < 3.0.35 / 3.2.13 / 3.3.6 Multiple Vulnerabilities Upgrade to Samba version 3.3.6 / 3.2.13 / 3.0.35 or later, or apply the appropriate patch referenced in the vendor's advisory.		☐
SAMBA 3.0 < 3.0.35 Upgrade to the latest version of Samba 3.0. Please see: http://www.samba.org		☐
Samba < 3.0.28 Multiple Vulnerabilities Upgrade to Samba version 3.0.28 or later. Please see: http://www.samba.org		☐
SMB Host SID Informational plugin.		☐
Microsoft Windows SMB Shares Unprivileged Access To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing'		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
tab, and click on 'permissions'.		
SMB NULL Session Disable the use of SMB Null Sessions, should it not be a business requirement.		☐
Outdated SSH Protocol Versions Supported If you use OpenSSH, set the option 'Protocol' to '2'. If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.		☐
SSH Protocol Versions Supported. Informational plugin.		☐
WINS Domain Controller Spoofing Vulnerability The following workaround was provided by David Byrne : The best workaround I could think of is to use static entries for records that are sensitive (there are probably more besides 1Ch). Domain Controllers shouldn't be changed very often, so the management work would be minimal. The following workaround was provided by Paul L Schmehl : MS's response was that because WINS uses NetBIOS, which has no security capabilities, there was no way to prevent that sort of hijacking. Their answer is Active Directory, Kerberos and DNS.		☐
BIND 9 Denial of Service Vulnerabilities		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
Upgrade to BIND 9.4.0b2 / 9.3.3rc2 / 9.3.2-P1 / 9.2.7rc2 / 9.2.6-P1 or later. Please see: http://www.isc.org		
Sendmail < 8.13.2 Mail X-Header Handling Remote Overflow No suggestion at this time		☐
Samba < 3.0.30 Multiple Vulnerabilities Upgrade to Samba version 3.0.30. Please see: http://www.samba.org		☐
MS00-047: NetBIOS Name Server Protocol Spoofing patch (269239) No suggestion at this time		☐
ProFTPD Command Truncation Cross-Site Request Forgery No suggestion at this time		☐
[DSA1218] DSA-1218-1 proftpd No suggestion at this time		☐
Usable Remote Name Server Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8 you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf. If you are using another name		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
server consult its documentation.		
DNS Amplification Restrict access to your DNS server from public network or reconfigure it to reject such queries.		☐
Disabled SMB Signing Workaround: Please refer to Microsoft's article 887429 for information on enabling SMB signing.		☐
UDP Constant IP Identification Field Fingerprinting Vulnerability We are not currently aware of any fixes for this issue.		☐
FTP Supports Clear Text Authentication Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.		☐
Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities Upgrade to Samba 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 or later.		☐
ISC BIND 9 EVP_VerifyFinal() / DSA_do_verify() SSL/TLS Signature Validation Weakness Upgrade to BIND 9.3.6-P1 / 9.4.3-P1 / 9.5.1-P1 / 9.6.0-P1 or later.		☐

192.168.235.56 : Recommendations

Recommendations	Comments	Completed
OpenSSH X11 Session Hijacking Vulnerability Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org		☐
ISC BIND 9 DNSSEC Cache Poisoning No suggestion at this time		☐
ISC BIND Dynamic Update Message Handling Remote DoS No suggestion at this time		☐
TCP Sequence Number Approximation Please see http://www.securityfocus .com/bid/10183/solution, for the right solution for your infrastructure.		☐
[DSA1164] DSA-1164-1 sendmail No suggestion at this time		☐
ProFTPd User Enumeration Update software to newest version. Please see: http://www.proftpd.org		☐

192.168.235.57 : Recommendations

Recommendations	Comments	Completed
OpenSSH < 5.0 Upgrade to the latest version of OpenSSH. Please see: www.openssh.org		☐
Multiple Linux Vendor rpc.statd Remote Format String Vulnerability mmoSuggestion Upgrade to the latest version of rpc.statd (see references)		☐
OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org		☐
UDP packets with source port of 53 bypass firewall rules Review your firewall rules policy and ensure that your firewall is stateful (tracks the state of allowed connections).		☐
TCP Sequence Number Approximation Please see http://www.securityfocus .com/bid/10183/solution, for the right solution for your infrastructure.		☐
SSH Protocol Versions Supported. Informational plugin.		☐
Hidden RPC Services Firewalling the portmapper port or		☐

192.168.235.57 : Recommendations

Recommendations	Comments	Completed
removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.		
OpenSSH X11 Session Hijacking Vulnerability Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org		☐

192.168.235.58 : Recommendations

Recommendations	Comments	Completed
Mail Relaying Allowed Configure your SMTP server so that it can't be used as a relay any more.		☐
MS04-035: Microsoft SMTP Remote Code Execution Microsoft has released a patch to fix this vulnerability. More information can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx		☐
MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check) Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx		☐
Microsoft Outlook Web Access 2003 vulnerable to URL Injection. The vendor has addressed this issue in Exchange 2007. Contact the vendor for details.		☐
Microsoft Outlook Web Access 2003 vulnerable to URL Injection. The vendor has addressed this issue in Exchange 2007. Contact the vendor for details.		☐
HTTP Basic Logins Sent Over Unencrypted Connection		☐

192.168.235.58 : Recommendations

Recommendations	Comments	Completed
Recommendations include ensuring that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted.		
SSL Certificate Expiry Apply for a new certificate from your preferred Certificate Authority or PKI.		☐
FTP Supports Clear Text Authentication Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.		☐
AutoComplete Attribute Not Disabled for Password in Form Based Authentication Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.		☐
Firewall Enabled Informational plugin.		☐
AutoComplete Attribute Not Disabled for Password in Form Based Authentication Contact the vendor to have the		☐

192.168.235.58 : Recommendations

Recommendations	Comments	Completed
AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.		
Windows Service Pack Level Appears Outdated Ensure that the server is running the latest stable Windows Service Pack. Please note also that Windows NT4.0 is no longer being supported by Microsoft. NT4.0 users are encouraged to upgrade to Windows 2000 or Windows 2003.		☐
Windows Service Pack Level Appears Outdated Ensure that the server is running the latest stable Windows Service Pack. Please note also that Windows NT4.0 is no longer being supported by Microsoft. NT4.0 users are encouraged to upgrade to Windows 2000 or Windows 2003.		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
SQL Injection (confirmed) Use the following recommendations to code web applications that are not susceptible to SQL Injection attacks. i) Parametrized Queries: SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed. The downside of this approach is that it can have an impact on performance, albeit slight, and that each query on the site must be structured in this method for it to be completely effective. If one query is inadvertently bypassed, that could be enough to leave the application vulnerable to SQL Injection. ii) Validate input: The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format. The best method of doing this is via "white listing". This is defined as only accepting specific account numbers or specific account types for those relevant fields, or only accepting integers or letters of the English alphabet for others. Many developers will try to validate input by "black listing" characters, or "escaping" them. Basically, this entails rejecting known bad data, such as a single quotation mark, by placing an "escape" character in front of it so that the item that follows will be treated as a literal value. This approach is not as effective as white listing because it is		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
impossible to know all forms of bad data ahead of time.		
SQL Injection Confirmed (No Data Extraction) There are two ways to mitigate the possibility of SQL Injection attacks: i) Parametrized Queries: SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injection attacks is thereby to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed. The downside of this approach is that it can have an impact on performance, albeit slight, and that each query on the site must be structured in this method for it to be completely effective. If one query is inadvertently bypassed, that could be enough to leave the application vulnerable to SQL Injection. ii) Validate input: The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format. The best method of doing this is via "white listing". This is defined as only accepting specific account numbers or specific account types for those relevant fields, or only accepting integers or letters of the English alphabet for others. Many developers will try to validate input by "black listing" characters, or "escaping" them. Basically, this entails rejecting known bad data, such as a single quotation mark, by placing an "escape" character in front of it		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
so that the item that follows will be treated as a literal value. This approach is not as effective as white listing because it is impossible to know all forms of bad data ahead of time.		
Blind SQL Injection (confirmed) Recommendations include employing a layered approach to security that includes utilizing parameterized queries when accepting user input, ensuring that only expected data is accepted by an application, and hardening the database server to prevent data from being accessed inappropriately.		☐
Database Server Error Message From a development perspective, the best method of limiting vulnerabilities arising from error message displays, is to adopt secure programming techniques that will prevent an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that. - Stringently define the data type that the application will accept. - Validate input in such a way to filter out improper characters. - Do not display error messages in a way that could be utilized in orchestrating an attack. - Define the allowed set of characters. - Define the maximum and minimum data lengths for what the application will accept. - Specify acceptable numeric ranges for input.		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
Cross-Site Scripting Cross-Site Scripting attacks can be avoided by carefully validating all input, and properly encoding all output. Validation can be done using standard ASP.NET Validation controls, or directly in your code. Always use the most stringent pattern possible. Encoding of output ensures that any scriptable content is properly encoded for HTML before being sent to the client. This is done with the function HttpUtility.HtmlEncode, as shown in the following Label control sample: Label2.Text = HttpUtility.HtmlEncode(input) Be sure to consider all paths that user input takes through your application. For instance, if data is entered by the user, stored in a database, and then redisplayed later, you must make sure it is properly encoded each time it is retrieved. If you must allow free-format text input, such as in a message board, and you wish to allow some HTML formatting to be used, you can handle this safely by explicitly allowing only a small list of safe tags.		☐
PHP < 5.2.9 Multiple Vulnerabilities Upgrade to PHP version 5.2.9 or later. Please see: http://www.php.net		☐
PHP < 5.2.5 Multiple Vulnerabilities Upgrade to PHP version 5.2.5 or		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
later. Please see: http://www.php.net		
mod_ssl < 2.8.31 Upgrade to the latest version of mod_ssl. Please see: http://www.modssl.org/		☐
PHP < 5.2.6 Multiple Vulnerabilities Upgrade to PHP version 5.2.6 or later. Please see: http://www.php.net		☐
PHP < 5.2 Multiple Vulnerabilities Upgrade to PHP version 5.2.0 or later. Please see: http://www.php.net		☐
PHP < 5.2.4 Multiple Vulnerabilities Upgrade to PHP version 5.2.4 or later. Please see: http://www.php.net		☐
PHP < 5.2.1 Multiple Vulnerabilities Upgrade to PHP version 5.2.1 or later. Please see: http://www.php.net		☐
OpenSSL 0.9 < 0.9.8k Upgrade to the latest version of OpenSSL. Please see http://www.openssl.org		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
PHP 5 < 5.2.7 Multiple Vulnerabilities Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.		☐
PHP < 4.4.7 / 5.2.2 Multiple Vulnerabilities Upgrade to PHP 4.4.7 / 5.2.2 or later. Please see: http://www.php.net		☐
MySQL < 5.1 Upgrade to the latest version of MySQL. Please see: http://dev.mysql.org		☐
PHP < 5.2.3 Multiple Vulnerabilities Upgrade to PHP version 5.2.3 or later. Please see: http://www.php.net		☐
PHP cURL "safe_mode" and "open_basedir" Restriction Bypass Vulnerability Avoid the use of "safe_mode" and "open_basedir" as main security functions. Patch: There are no vendor-supplied patches available at this time. For the latest updates visit the PHP		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
Web site.		
Unencrypted Login Form Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. A page containing a login form should be sent over SSL as well as the Action of the form. This will prevent Man-in-the-Middle attacks on the login form.		☐
Logins Sent Over Unencrypted Connection Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data from being intercepted.		☐
PHP Nested Array Denial Of Service Recommendations include upgrading to a fixed version of PHP.		☐
Password in Query Data The process to login should be changed to allow for login information to be sent with POST data over an encrypted connection.		☐
PHP "dba_replace()" File Corruption Vulnerability Upgrade to the latest version of PHP.		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
MySQL Community Server 5.0 < 5.0.67 Multiple Vulnerabilities Upgrade to MySQL Community Server version 5.0.67.		☐
Apache < 2.2.8 Multiple Vulnerabilities Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.		☐
Apache < 2.2.6 Multiple Vulnerabilities Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.6 or later.		☐
MySQL Community Server 5.0 < 5.0.51 RENAME TABLE Symlink System Table Overwrite Upgrade to MySQL Community Server version 5.0.51 or later.		☐
Apache 2.2 < 2.2.14 Multiple Vulnerabilities Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.		☐
Apache < 2.2.9 Multiple Vulnerabilities Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.		☐
		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
MySQL Community Server 5.0 < 5.0.51 RENAME TABLE Symlink System Table Overwrite Upgrade to MySQL Community Server version 5.0.51 or later.		
MySQL Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial of Service Vulnerability There are no vendor-supplied patches available at this time.		☐
UDP packets with source port of 53 bypass firewall rules Review your firewall rules policy and ensure that your firewall is stateful (tracks the state of allowed connections).		☐
Directory Listing Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application. i) Restrict access to important files or directories only to those who actually need it. ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
best left confidential.		
Script Name/Path Parameter Cross-Site Scripting Recommendations include modifying source code to properly validate input parameters or updating to a fixed version of the application.		☐
Possible File Upload Capability Recommendations include adopting a strict file upload policy that prevents malicious material from being uploaded via sanitization and filtering.		☐
PHP Version Information Disclosure Recommendations include setting expose_php to Off in your php.ini configuration file.		☐
HTTP TRACE/TRACK Methods Supported If you are using Apache, add the following lines for each virtual host in your configuration file:;; RewriteEngine on; RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK); RewriteRule .* - [F];; If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.		☐
Exception Error Message Recommendations include designing and adding consistent error-		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.		
NetBIOS Name Service Reply Information Leakage Download patch from http://www.microsoft.com/technet/security/bulletin/ms03-034.asp		☐
PHP 'popen()' Function Buffer Overflow Vulnerability There are no vendor-supplied patches available at this time. For the latest information, visit the PHP Web site.		☐
MySQL Crafted IF Clause Divide-by-zero NULL Dereference DoS Upgrade to MySQL Community Server 5.0.41 / 5.1.18 / Enterprise Server 5.0.40 or later.		☐
MySQL Single Row Subselect Remote DoS Upgrade to MySQL version 5.0.37 or newer.		☐
Apache 2.x < 2.2.12 Multiple Vulnerabilities Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
MySQL Enterprise Server 5.0 < 5.0.66 Empty Bit-String Literal Token SQL Statement DoS No suggestion at this time		☐
MySQL 5.1 < 5.1.32 XPath Expression DoS No suggestion at this time		☐
MySQL Community Server 5.0 < 5.0.45 Multiple Vulnerabilities Upgrade to MySQL Community Server version 5.0.45 or later.		☐
PHP < 5.2.10 Multiple Vulnerabilities Upgrade to PHP version 5.2.10 or later. Please see: http://www.php.net		☐
MySQL 5.1 < 5.1.18 Multiple Vulnerabilities No suggestion at this time		☐
Apache 2.2 < 2.2.11 Upgrade to the latest version of Apache 2.2. Please see: http://httpd.apache.org		☐
PHP < 5.2.11 Multiple Vulnerabilities Upgrade to PHP version 5.2.11 or later.		☐

192.168.235.59 : Recommendations

Recommendations	Comments	Completed
MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability MYSQL has released a patch to address this issue. Refer to MySQL Bug #27884 for further details on these vulnerabilities and patch instructions.		☐
PHP 'mbstring.func_overload' Webserver Denial of Service Vulnerability Upgrade to the latest version of PHP.		☐
PHP 5.3 < 5.3.1 Multiple Vulnerabilities No suggestion at this time		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Open X11 Server Restrict access to this port by using the 'xhost' command. If the X11 client/server facility is not used, disable TCP entirely.		☐
SNMP Weak / Guessable Community String SNMP should preferably be removed if not in use.;; Alternatively, the following security precautions should be put in place:; - All community strings should be set to stronger, less easily guessable alternatives.; - If SNMP is only used for monitoring purposes, write access should be disabled.; - SNMP enabled hosts should be configured to only accept SNMP traffic from authorised IP addresses or network ranges, such as the Network Management Segment (NMS).; - Wherever possible SNMP version 3 should be used, as it provides for better authentication and encryption, ensuring community strings for example do not traverse the network in the clear.;; For Windows 2000 and 2003 SNMP settings can be configured through the SNMP Security Properties tab:; Administrative Tools >> Computer Management >> Services and Applications >> Services >> SNMP Service >> right click, select Properties >> Security.;		☐
Buffer Overflow in CDE Subprocess Control Service		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Solution : See http://www.cert.org/advisories/CA-2001-31.html to determine if you are vulnerable or deactivate this service (comment out the line 'dtspc' in /etc/inetd.conf and restart the inetd process).		
Solaris 10 Telnet Authentication Bypass It is recommended that telnet not be used and instead replaced with SSH. Should SSH not be a viable option, implementing the vendor supplied patch is recommended. The vendor supplied patches are: 120068-02 (sparc) 120069-02 (i386)		☐
Apache Tomcat JK Web Server Connector Buffer Overflow Recommendations include upgrading to the latest version.		☐
Apache Tomcat JK Web Server Connector Buffer Overflow Recommendations include upgrading to the latest version.		☐
X Display Manager Control Protocol (XDMCP) Disable the XDMCP if you do not use it, and do not allow this service to run across the Internet		☐
Dangerous Service: rlogin You should disable this service in /etc/inetd.conf.		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Sun Java Web Console Navigator Cross Site Scripting There are no vendor-supplied patches available at this time.		☐
Sun Java Web Console Navigator Cross Site Scripting There are no vendor-supplied patches available at this time.		☐
Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.		☐
Sun Java Web Console LibWebconsole_Services.SO Remote Format String No suggestion at this time		☐
Sun Java Web Console masthead.jsp Cross-Site Scripting There are no vendor-supplied patches available at this time.		☐
Multiple Vendor CDE ToolTalk Database Server Null Write Vulnerability Please contact your vendor for patch information.		☐
Sun Java Web Console masthead.jsp Cross-Site Scripting		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
There are no vendor-supplied patches available at this time.		
Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.		☐
Unencrypted Telnet Server Disable this service and use SSH instead.		☐
Administrative Directories Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.		☐
FTP Supports Clear Text Authentication Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such as data and control connections must be encrypted.		☐
Directory Listing Unless you are actively involved with implementing the web		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application. i) Restrict access to important files or directories only to those who actually need it. ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.		
SSL Certificate Signed using Weak Hashing Algorithm Contact the Certificate Authority to have the certificate reissued.		☐
TCP Sequence Number Approximation Please see http://www.securityfocus .com/bid/10183/solution, for the right solution for your infrastructure.		☐
SSL Medium Strength Cipher Suites Supported Reconfigure the affected application if possible to avoid use of medium strength ciphers.		☐
Administrative Directories Recommendations include restricting access to important directories or		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.		
Finger zero at host Information Disclosure Vulnerability Filter access to this port, upgrade the finger server, or disable it entirely.		☐
Directory Listing Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application. i) Restrict access to important files or directories only to those who actually need it. ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.		☐
Global User List To prevent your host from being attacked, do one or more of the following:		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Remove (or rename) unnecessary accounts Shutdown unnecessary network services Ensure the passwords to these accounts are kept secret Use a firewall to restrict access to your hosts from unauthorized domains		
EXPN and VRFY commands EXPN and VRFY should be disabled on the mail server.		☐
Weak Supported SSL Ciphers Suites Reconfigure the affected application if possible to avoid use of weak ciphers.		☐
Hidden RPC Services Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.		☐
Dangerous Service: rsh You should disable this service and use ssh instead. To disable the service comment out the 'rsh' line in /etc/inetd.conf.		☐
Sun Java Web Console May Allow Unauthorized Redirection (243786) This issue has been addressed in the following releases:		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
SPARC Platform: Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later Solaris 10 with patch 125952-18 or later x86 Platform: Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later Solaris 10 with patch 125953-18 or later Linux Platform: Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later Windows: Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.		
Sun Java Web Console May Allow Unauthorized Redirection (243786) This issue has been addressed in the following releases: SPARC Platform: Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136987-02 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125950-18 or later Solaris 10 with patch 125952-18 or		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
later x86 Platform: Sun Java Web Console 3.0.2 (for Solaris 8) with patch 136986-02 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 (for Solaris 9) with patch 125951-18 or later Solaris 10 with patch 125953-18 or later Linux Platform: Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 with patch 125954-18 or later Windows: Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 bundled with JES with patch 125955-18 or later Sun Java Web Console 3.0.2, 3.0.3, 3.0.4, 3.0.5 unbundled from JES with patch 127534-18 or later Refer to Sun Alert ID 243786 to obtain additional information on this vulnerability and patch details.		
Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability Refer to this Apache Tomcat Web site for details about the latest versions.		☐
Apache Tomcat Information Disclosure Vulnerability The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.		☐
Apache Tomcat Servlet Host Manager Servlet Cross-Site Scripting Vulnerability		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Refer to this Apache Tomcat Web site for details about the latest versions.		
Sendmail Long Header Denial Of Service Vulnerability Upgrade to version 8.13.8 or greater.		☐
Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications Refer to this Apache Tomcat Web site for details about the latest versions.		☐
Sun Java Web Console < 3.0.5 Remote File Enumeration Apply the appropriate patch as discussed in the vendor advisory: h ttp://sunsolve.sun.com/search/docum ent.do?assetkey=1-26-231526-1		☐
Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications Refer to this Apache Tomcat Web site for details about the latest versions.		☐
Sun Java Web Console helpwindow.jsp Cross Site Scripting There are no vendor-supplied patches available at this time.		☐

192.168.235.60 : Recommendations

Recommendations	Comments	Completed
Sun Java Web Console helpwindow.jsp Cross Site Scripting There are no vendor-supplied patches available at this time.		☐
Apache Tomcat Information Disclosure Vulnerability The vendor has released fixes to address these issues. Refer to this Apache Tomcat security page for patch and update information.		☐
Sun Java Web Console < 3.0.5 Remote File Enumeration Apply the appropriate patch as discussed in the vendor advisory: h ttp://sunsolve.sun.com/search/docum ent.do?assetkey=1-26-231526-1		☐
Apache Tomcat Multiple Content Length Headers Information Disclosure Vulnerability Refer to this Apache Tomcat Web site for details about the latest versions.		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
OpenSSH Buffer Management Vulnerability (OpenSSH < 3.7.1) This issue is resolved in OpenSSH releases 3.7.1 and later. Upgrade to latest stable release version of OpenSSH available from www.openssh.com. Manual patches for this issue are available from http://www.openssh.com/txt/buffer.adv. For vendor specific patch information, look up the vendor in question from http://www.securityfocus.com/bid/8628/solution, or contact the vendor directly.		☐
OpenSSH < 5.0 Upgrade to the latest version of OpenSSH. Please see: www.openssh.org		☐
OpenSSH < 4.0 Upgrade to the latest version of OpenSSH. Please see: www.openssh.org		☐
OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities Upgrade to OpenSSH 4.4 or later. Please see: http://www/openssh.org		☐
SuSE Security Update: libapr-util1 (2009-10-11) No suggestion at this time		☐
Outdated SSH Protocol Versions Supported		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
If you use OpenSSH, set the option 'Protocol' to '2'. If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'.		
Default Password: Guest Account Set a password for this account or disable it		☐
OpenSSH Reverse DNS Lookup bypass Upgrade to the latest stable release version of OpenSSH, available from http://www.openssh.org. This problem is resolved in OpenSSH 3.6.2 and later.		☐
Apache < 2.2.9 Multiple Vulnerabilities Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.		☐
Apache < 2.2.8 Multiple Vulnerabilities Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.		☐
Apache 2.2 < 2.2.14 Multiple Vulnerabilities Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.		☐
Apache < 2.2.6 Multiple Vulnerabilities		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.6 or later.		
Apache < 2.2.3 Upgrade to the latest version of Apache. Please see: http://httpd.apache.org		☐
UDP Constant IP Identification Field Fingerprinting Vulnerability We are not currently aware of any fixes for this issue.		☐
Directory Listing Unless you are actively involved with implementing the web application server, there is not a wide range of available solutions to prevent problems that can occur from an attacker finding a Directory Listing. Primarily, this problem will be resolved by the web application server administrator. However, there are certain actions you can take that will help to secure your web application. i) Restrict access to important files or directories only to those who actually need it. ii) Ensure that files containing sensitive information are not left publicly accessible, or that comments left inside files do not reveal the locations of directories best left confidential.		☐
Hidden RPC Services Firewalling the portmapper port or		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.		
HTTP TRACE/TRACK Methods Supported If you are using Apache, add the following lines for each virtual host in your configuration file:;; RewriteEngine on; RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK); RewriteRule .* - [F];; If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.		☐
TCP Sequence Number Approximation Please see http://www.securityfocus .com/bid/10183/solution, for the right solution for your infrastructure.		☐
Apache HTTP Server OS Fingerprinting Unspecified Security Vulnerability Upgrade to the latest version of Apache 2.2, which is available for download from the Apache Web site.		☐
Apache 2.x < 2.2.12 Multiple Vulnerabilities Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
Apache 2.2 < 2.2.11 Upgrade to the latest version of Apache 2.2. Please see: http://httpd.apache.org		☐
OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056) If you are a Fedora user, please visit Fedora advisory FEDORA-2006-056. HP has released a patch to address this issue. Refer to HP's technical support document HPSBUX02178 (registration required) for further details. Open SSH release release-4.3 fixes the issue. Please visit OpenSSH release-4.3 Web site for more information on updates. You can confirm if this vulnerability is present on your computer as follows. On a Unix prompt, type these commands: a. touch foo bar b. mkdir "any_directory" c. scp foo bar "any_directory" If the output is: "cp: cannot stat `foo': No such file or directory cp: cannot stat `bar': No such file or directory" then your OpenSSH is vulnerable. Refer to the following link for Redhat advisoryRHSA-2006:0044-14. Refer to Vmware advisoryVMware Patch 9986131, yVMware Patch 3069097.		☐
OpenSSH X11 Session Hijacking Vulnerability		☐

192.168.235.61 : Recommendations

Recommendations	Comments	Completed
Upgrade to OpenSSH version 5.0 or later. Please see: http://www/openssh.org		
Apache mod_proxy_ftp Globbing Cross-Site Scripting Vulnerability Either disable the affected module or upgrade to Apache version 2.2.10 or later.		☐
Apache Partial HTTP Request Denial of Service Vulnerability - Zero Day Patch: There are no vendor-supplied patches available at this time. Workaround: -Reverse proxies, load balancers and iptables can help to prevent this attack from occurring. -Adjusting the TimeOut Directive can also prevent this attack from occurring.		☐