OpenVAS Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	6
Number of security holes found	11
Number of security warnings found	26
Number of security notes found	110
Number of false positives found	0

Host List

Host(s)	Possible Issue
192.168.1.110	Security hole(s) found
192.168.1.111	Security warning(s) found
192.168.1.112	Security note(s) found
192.168.1.113	Security hole(s) found
192.168.1.114	Security warning(s) found
192.168.1.115	Security hole(s) found

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.110	smtp (25/tcp)	Security note(s) found
192.168.1.110	http (80/tcp)	Security hole(s) found
192.168.1.110	epmap (135/tcp)	Security warning(s) found
192.168.1.110	netbios-ssn (139/tcp)	Security note(s) found
192.168.1.110	https (443/tcp)	No Information
192.168.1.110	microsoft-ds (445/tcp)	Security note(s) found
192.168.1.110	blackjack (1025/tcp)	Security note(s) found
192.168.1.110	cap (1026/tcp)	Security note(s) found
192.168.1.110	exosee (1027/tcp)	Security note(s) found
192.168.1.110	tip2 (3372/tcp)	No Information
192.168.1.110	general/tcp	Security note(s) found
192.168.1.110	ssh (22/tcp)	No Information
192.168.1.110	netbios-ns (137/udp)	Security warning(s) found
192.168.1.110	general/SMB	Security note(s) found
192.168.1.110	ms-lsa (1028/udp)	Security note(s) found
192.168.1.110	iad1 (1030/udp)	Security note(s) found
192.168.1.110	general/SMBClient	Security note(s) found

Security Issues and Fixes: 192.168.1.110

Type	Port	Issue and Fix
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 training1 Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Thu, 2 Jul 2009 12:41:53 +1000 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 training1 Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Thu, 2 Jul 2009 12:42:26 +1000

This is probably: Microsoft Exchange version 5.0.2172.1 ready at Thu, 2 Jul

		2009 12:42:26 +1000 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10263
Vulnerability	http (80/tcp)	The remote IIS server allows anyone to execute arbitrary commands by adding a unicode representation for the slash character in the requested path. Solution: See http://www.microsoft.com/technet/security/bulletin/ms00-078.mspx Risk factor : High CVE : CVE-2000-0884 BID : 1806 Other references : IAVA:2000-a-0005 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10537
Warning	http (80/tcp)	This IIS Server appears to vulnerable to one of the cross site scripting attacks described in MS02-018. The default '404' file returned by IIS uses scripting to output a link to top level domain part of the url requested. By crafting a particular URL it is possible to insert arbitrary script into the page for execution. The presence of this vulnerability also indicates that you are vulnerable to the other issues identified in MS02-018 (various remote buffer overflow and cross site scripting attacks...) References: http://www.microsoft.com/technet/security/bulletin/MS02-018.mspx http://jscript.dk/adv/TL001/ Risk factor : Medium CVE : CVE-2002-0148, CVE-2002-0150 BID : 4476, 4483, 4486 Other references : IAVA:2002-A-0002 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10936
Warning	http (80/tcp)	IIS 4.0 allows a remote attacker to obtain the real pathname of the document root by requesting non-existent files with .ida or .idq extensions. An attacker may use this flaw to gain more information about the remote host, and hence make more focused attacks. Solution: Select 'Preferences ->Home directory ->Application', and check the checkbox 'Check if file exists' for the ISAPI mappings of your server. Risk factor : Low CVE : CVE-2000-0071 BID : 1065 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10492
Informational	http (80/tcp)	A web server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	http (80/tcp)	The remote web server type is : Microsoft-IIS/5.0 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107
Informational	http (80/tcp)	Synopsis : Debugging functions are enabled on the remote HTTP server. Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution :

		Disable these methods. See also : http://www.kb.cert.org/vuls/id/867593 Risk factor : Low / CVSS Base Score : 2 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N) Plugin output : Solution : Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. CVE : CVE-2004-2320 BID : 9506, 9561, 11604 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11213
Informational	http (80/tcp)	The following directories were discovered: /_vti_bin, /images 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: /printers Other references : OWASP:OWASP-CM-006 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11032
Informational	http (80/tcp)	The remote IIS server *seems* to be Microsoft IIS 5 - SP0 or SP1 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11874
Informational	http (80/tcp)	Synopsis : Indexing Service filter is enabled on the remote Web server. Description : The IIS server appears to have the .IDA ISAPI filter mapped. At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033, and gives remote SYSTEM level access to the web server. It is recommended that even if you have patched this vulnerability that you unmap the .IDA extension, and any other unused ISAPI extensions if they are not required for the operation of your site. Solution : To unmap the .IDA extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .ida from the list. In addition, you may wish to download and install URLSCAN from the Microsoft Technet web site. URLSCAN, by default, blocks all .ida requests to the IIS server. Risk factor : None / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) CVE : CVE-2001-0500 BID : 2880 Other references : IAVA:2001-a-0008 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10695
Informational	http (80/tcp)	\nServer: Microsoft-IIS/5.0\nOperating System Type: Windows Server 2000 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.101018
Informational	http (80/tcp)	Synopsis : Remote Web server supports Internet Printing Protocol

		Description : IIS 5 has support for the Internet Printing Protocol(IPP), which is enabled in a default install. The protocol is implemented in IIS5 as an ISAPI extension. At least one security problem (a buffer overflow) has been found with that extension in the past, so we recommend you disable it if you do not use this functionality. Solution : To unmap the .printer extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration and remove the reference to .printer from the list. See also : http://online.securityfocus.com/archive/1/181109 Risk factor : None / CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10661
Warning	epmap (135/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	netbios-ssn (139/tcp)	An SMB server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	A CIFS server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	It was possible to log into the remote host using user defined login/password combinations : OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10394
Informational	blackjack (1025/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1025] UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1025] UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1025] UUID: 906b0ce0-c70b-1067-b317-00dd010662da, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1025] Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	cap (1026/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate

		queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1026] Named pipe : atsvc Win32 service or process : mstask.exe Description : Scheduler service UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1026] Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	exosee (1027/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2 Endpoint: ncacn_ip_tcp:192.168.1.110[1027] UUID: 8cfb5d70-31a4-11cf-a7d8-00805f48a135, version 3 Endpoint: ncacn_ip_tcp:192.168.1.110[1027] UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1 Endpoint: ncacn_ip_tcp:192.168.1.110[1027] Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	general/tcp	ICMP based OS fingerprint results: Microsoft Windows 2003 Server Enterprise Edition (accuracy 95%) Microsoft Windows 2003 Server Standard Edition (accuracy 95%) Microsoft Windows XP SP2 (accuracy 95%) Microsoft Windows XP SP1 (accuracy 95%) Microsoft Windows XP (accuracy 95%) Microsoft Windows 2000 Server Service Pack 4 (accuracy 95%) Microsoft Windows 2000 Server Service Pack 3 (accuracy 95%) Microsoft Windows 2000 Server Service Pack 2 (accuracy 95%) Microsoft Windows 2000 Server Service Pack 1 (accuracy 95%) Microsoft Windows 2000 Server (accuracy 95%) Microsoft Windows 2000 Workstation SP4 (accuracy 95%) Microsoft Windows 2000 Workstation SP3 (accuracy 95%) Microsoft Windows 2000 Workstation SP2 (accuracy 95%) Microsoft Windows 2000 Workstation SP1 (accuracy 95%) Microsoft Windows 2000 Workstation (accuracy 95%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002
Informational	general/tcp	Nikto could not be found in your system path. OpenVAS was unable to execute Nikto and to perform the scan you requested. Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.14260
Informational	general/tcp	Information about this scan : OpenVAS version : 2.0.1 Plugin feed version : 200906251300 Type of plugin feed : OpenVAS NVT Feed Scanner IP : 192.168.1.106

		Port scanner(s) : openvas_tcp_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan duration : unknown (ping_host.nasl not launched?) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506
Warning	netbios-ns (137/udp)	The following 5 NetBIOS names have been gathered : TRAINING1 WORKGROUP = Workgroup / Domain name TRAINING1 = This is the computer name WORKGROUP = Workgroup / Domain name (part of the Browser elections) TRAINING1 = This is the current logged in user or registered workstation name. The remote host has the following MAC address on its adapter : 00:0c:29:64:44:7b If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10150
Informational	general/SMB	WINNT\system32\Dnsapi.dll not found/no access -> CVE : CVE-2008-0087 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90020
Informational	general/SMB	WINNT\system32\Dnsapi.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2008-0087 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90020
Informational	general/SMB	.NET V2xx not found/no access -> Domain=[WORKGROUP] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-0043 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90010
Informational	general/SMB	.NET V2xx not found/no access -> CVE : CVE-2007-0043 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90010
Informational	general/SMB	WINNT\system32\Msjint40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINNT\system32\Msjet40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINNT\system32\Msjet40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINNT\system32\Msjint40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINNT\system32\Msjet40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINNT\system32\Msjet40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager] tree connect failed: NT_STATUS_ACCESS_DENIED

		CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	ms-lsa (1028/udp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: bfa951d1-2f0e-11d3-bfd1-00c04fa3490a, version 1 Endpoint: ncadg_ip_udp:192.168.1.110[1028] Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	iad1 (1030/udp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1 Endpoint: ncadg_ip_udp:192.168.1.110[1030] Annotation: Messenger Service Named pipe : ntsvcs Win32 service or process : messenger Description : Messenger service Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	general/SMBClient	OS Version = WINDOWS 5.0 Domain = WORKGROUP SMB Serverversion = WINDOWS 2000 LAN MANAGER OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90011

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.111	epmap (135/tcp)	Security warning(s) found
192.168.1.111	netbios-ssn (139/tcp)	Security note(s) found
192.168.1.111	microsoft-ds (445/tcp)	Security note(s) found
192.168.1.111	blackjack (1025/tcp)	Security note(s) found
192.168.1.111	general/tcp	Security note(s) found
192.168.1.111	ssh (22/tcp)	No Information
192.168.1.111	netbios-ns (137/udp)	Security warning(s) found
192.168.1.111	general/SMB	Security note(s) found
192.168.1.111	general/SMBClient	Security note(s) found

Security Issues and Fixes: 192.168.1.111

Type	Port	Issue and Fix
Warning	epmap (135/tcp)	Distributed Computing Environment (DCE) services running on the remote host

		can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	netbios-ssn (139/tcp)	An SMB server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	A CIFS server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11011
Informational	microsoft-ds (445/tcp)	It was possible to log into the remote host using user defined login/password combinations : OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10394
Informational	blackjack (1025/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.1.111[1025] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.1.111[1025] Annotation: IPSec Policy agent endpoint Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service Solution : filter incoming traffic to this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10736
Informational	general/tcp	ICMP based OS fingerprint results: Microsoft Windows 2003 Server Enterprise Edition (accuracy 100%) Microsoft Windows 2003 Server Standard Edition (accuracy 100%) Microsoft Windows XP SP2 (accuracy 100%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002
Informational	general/tcp	Synopsis : The remote service implements TCP timestamps. 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 sometimes be computed. See also : http://www.ietf.org/rfc/rfc1323.txt Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.80091
Informational	general/tcp	Information about this scan : OpenVAS version : 2.0.1 Plugin feed version : 200906251300

		Type of plugin feed : OpenVAS NVT Feed Scanner IP : 192.168.1.106 Port scanner(s) : openvas_tcp_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan duration : unknown (ping_host.nasl not launched?) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506
Warning	netbios-ns (137/udp)	The following 6 NetBIOS names have been gathered : WIN2K3 = This is the computer name registered for workstation services by a WINS client. WORKGROUP = Workgroup / Domain name WIN2K3 = Computer name WORKGROUP = Workgroup / Domain name (part of the Browser elections) WORKGROUP __MSBROWSE__ The remote host has the following MAC address on its adapter : 00:0c:29:e2:36:75 If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10150
Informational	general/SMB	WINDOWS\system32\Dnsapi.dll not found/no access -> CVE : CVE-2008-0087 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90020
Informational	general/SMB	WINDOWS\system32\Dnsapi.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server= [Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2008-0087 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90020
Informational	general/SMB	.NET V2xx not found/no access -> Domain=[WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server=[Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-0043 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90010
Informational	general/SMB	.NET V2xx not found/no access -> CVE : CVE-2007-0043 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90010
Informational	general/SMB	WINDOWS\system32\drivers\mrxdav.sys not found/no access -> Domain= [WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server= [Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2008-0080 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90015
Informational	general/SMB	WINDOWS\system32\drivers\mrxdav.sys not found/no access -> CVE : CVE-2008-0080 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90015
Informational	general/SMB	WINDOWS\system32\Msjint40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server= [Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINDOWS\system32\Msjet40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server= [Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024

Informational	general/SMB	WINDOWS\system32\Msjet40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINDOWS\system32\Msjint40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINDOWS\system32\Msjet40.dll not found/no access -> CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMB	WINDOWS\system32\Msjet40.dll not found/no access -> Domain= [WORKGROUP] OS=[Windows Server 2003 3790 Service Pack 1] Server= [Windows Server 2003 5.2] tree connect failed: NT_STATUS_ACCESS_DENIED CVE : CVE-2007-6026 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90024
Informational	general/SMBClient	OS Version = WINDOWS SERVER 2003 3790 SERVICE PACK 1 Domain = WORKGROUP SMB Serverversion = WINDOWS SERVER 2003 5.2 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90011

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.112	daytime (13/tcp)	No Information
192.168.1.112	time (37/tcp)	Security note(s) found
192.168.1.112	http (80/tcp)	Security note(s) found
192.168.1.112	ident (113/tcp)	Security note(s) found
192.168.1.112	mysql (3306/tcp)	Security note(s) found
192.168.1.112	general/tcp	Security note(s) found
192.168.1.112	ssh (22/tcp)	No Information
192.168.1.112	general/SMBClient	No Information

Security Issues and Fixes: 192.168.1.112

Type	Port	Issue and Fix
Informational	time (37/tcp)	A time server seems to be running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	http (80/tcp)	A web server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	http (80/tcp)	The remote web server type is : Apache and the 'ServerTokens' directive is ProductOnly Apache does not permit to hide the server type. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107
Informational	ident (113/tcp)	An identd server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ident (113/tcp)	Overview: The remote host is running an ident daemon. The Ident Protocol is designed to work as a server daemon, on a user's computer, where it receives requests to a specified port, generally 113. The server will then send a specially designed response that identifies the username of the current user. The ident protocol is considered dangerous because it allows hackers to gain a list of usernames on a computer system which can later be used for attacks.

		Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100081
Informational	mysql (3306/tcp)	Overview: MySQL, a open source database system is running at this host. See also: http://www.mysql.com Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100152
Informational	general/tcp	ICMP based OS fingerprint results: NetBSD 1.5.3 (accuracy 95%) NetBSD 1.5.2 (accuracy 95%) NetBSD 1.5.1 (accuracy 95%) NetBSD 1.5 (accuracy 95%) NetBSD 1.4.3 (accuracy 95%) NetBSD 1.4.2 (accuracy 95%) NetBSD 1.4.1 (accuracy 95%) NetBSD 1.4 (accuracy 95%) OpenBSD 3.7 (accuracy 95%) OpenBSD 3.6 (accuracy 95%) OpenBSD 3.5 (accuracy 95%) OpenBSD 3.4 (accuracy 95%) OpenBSD 2.5 (accuracy 95%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002
Informational	general/tcp	Nikto could not be found in your system path. OpenVAS was unable to execute Nikto and to perform the scan you requested. Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.14260
Informational	general/tcp	Information about this scan : OpenVAS version : 2.0.1 Plugin feed version : 200906251300 Type of plugin feed : OpenVAS NVT Feed Scanner IP : 192.168.1.106 Port scanner(s) : openvas_tcp_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan duration : unknown (ping_host.nasl not launched?) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.113	http (80/tcp)	Security hole(s) found
192.168.1.113	https (443/tcp)	Security note(s) found
192.168.1.113	ntp-gps-data (12321/tcp)	Security note(s) found
192.168.1.113	ssh (22/tcp)	Security warning(s) found
192.168.1.113	ntp (123/udp)	Security note(s) found
192.168.1.113	general/tcp	Security note(s) found
192.168.1.113	general/SMBClient	No Information

Security Issues and Fixes: 192.168.1.113

Type	Port	Issue and Fix

Vulnerability http (80/tcp)

Overview: The host is installed with PHP, that is prone to multiple vulnerabilities.

Vulnerability Insight:
The flaws are caused by,
- an unspecified stack overflow error in FastCGI SAPI (fastcgi.c).
- an error during path translation in cgi_main.c.
- an error with an unknown impact/attack vectors.
- an unspecified error within the processing of incomplete multibyte characters in escapeshellcmd() API function.
- error in curl/interface.c in the cURL library(libcurl), which could be exploited by attackers to bypass safe_mode security restrictions.
- an error in PCRE. i.e buffer overflow error when handling a character class containing a very large number of characters with codepoints greater than 255(UTF-8 mode).

Impact:
Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.

Impact Level: System

Affected Software/OS:
PHP version prior to 5.2.6

Fix:
Upgrade to PHP version 5.2.6 or above,
http://www.php.net/downloads.php

References:
http://pcre.org/changelog.txt
http://www.php.net/ChangeLog-5.php
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086

CVSS Score:
CVSS Base Score : 9.0 (AV:N/AC:L/Au:NR/C:P/I:P/A:C)
CVSS Temporal Score : 7.0
Risk factor : High
CVE : CVE-2008-2050, CVE-2008-2051, CVE-2007-4850, CVE-2008-0599, CVE-2008-0674
BID : 29009, 27413, 27786
Other references : CB-A:08-0118
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800110

Vulnerability http (80/tcp)

Overview: The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Insight:
The flaw is caused due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Impact:
Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.

Impact Level: Application

Affected Software/OS:
PHP version 4.3.0 to 5.2.6 on all running platform.

Fix: Upgrade to version 5.2.7 or later,
http://www.php.net/downloads.php

References:
http://bugs.php.net/bug.php?id=45722
http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

CVSS Score:
CVSS Base Score : 10.0 (AV:N/AC:L/Au:NR/C:C/I:C/A:C)
CVSS Temporal Score : 7.4
Risk factor: High
CVE : CVE-2008-5557
BID : 32948
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900185

Vulnerability http (80/tcp)

Overview:
The host is running PHP and is prone to denial of service vulnerability.

Vulnerability Insight:
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server.

Impact:
Successful exploitation will let the local attackers to crash an affected web server.

Impact Level: Application

Affected Software/OS:
PHP version 4.4.4 and prior
PHP 5.1.x to 5.1.6
PHP 5.2.x to 5.2.5

Fix: No solution or patch is available as on 17th March, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, http://www.php.net

References:
http://bugs.php.net/bug.php?id=27421
https://bugzilla.redhat.com/show_bug.cgi?id=479272

CVSS Score:
CVSS Base Score : 2.1 (AV:L/AC:L/Au:NR/C:N/I:P/A:N)
CVSS Temporal Score : 1.9
Risk factor : Low
CVE : CVE-2009-0754
BID : 33542
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800373

Vulnerability http (80/tcp)

Overview: The host is running PHP and is prone to Security Bypass and File Writing vulnerability.

Vulnerability Insight:
The flaw is caused due to,
- An error in initialization of 'page_uid' and 'page_gid' global variables for use by the SAPI 'php_getuid' function, which bypass the safe_mode

restrictions.
- When 'safe_mode' is enabled through a 'php_admin_flag' setting in 'httpd.conf' file, which does not enforce the 'error_log', 'safe_mode restrictions.
- In 'ZipArchive::extractTo' function which allows attacker to write files via a ZIP file.

Impact:
Successful exploitation could allow remote attackers to write arbitrary file, bypass security restrictions and cause directory traversal attacks.

Impact Level: System/Application

Affected Software/OS:
PHP versions prior to 5.2.7.

Fix: Upgrade to version 5.2.7 or later
http://www.php.net/downloads.php

References:
http://www.php.net/ChangeLog-5.php#5.2.7
http://www.php.net/archive/2008.php#id2008-12-07-1
http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 5.9
Risk factor: High
CVE : CVE-2008-5624, CVE-2008-5625, CVE-2008-5658
BID : 32383, 32625, 32688
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900184

Vulnerability	http (80/tcp)	Overview : This host is running WordPress, which is prone to multiple vulnerabilities. Vulnerability Insight : The flaws are due to, - SQL column-truncation issue. - Weakness in the entropy of generated passwords. - functions get_edit_post_link(), and get_edit_comment_link() fail to use SSL when transmitting data. Impact : Successful exploitation will allow attackers to reset the password of arbitrary accounts, guess randomly generated passwords, obtain sensitive information and possibly to impersonate users and tamper with network data. Impact Level : Application Affected Software/OS : WordPress 2.6.1 and prior versions. Fix : Upgrade to WordPress 2.6.2 or later. http://wordpress.org/ References : http://www.sektioneins.de/advisories/SE-2008-05.txt http://seclists.org/fulldisclosure/2008/Sep/0194.html http://www.juniper.net/security/auto/vulnerabilities/vuln31068.html http://www.juniper.net/security/auto/vulnerabilities/vuln30750.html CVSS Score : CVSS Base Score : 6.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:P) CVSS Temporal Score : 5.3 Risk factor : High CVE : CVE-2008-3747 BID : 30750, 31068, 31115 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900219
Warning	http (80/tcp)	Overview: The host is installed with PHP and is prone to Denial of Service vulnerability. Vulnerability Insight: Improper handling of .zip file while doing extraction via php_zip_make_relative_path function in php_zip.c file. Impact:

		Successful exploitation could result in denial of service condition. Impact Level: Application Affected Software/OS: PHP version prior to 5.2.9 Fix: Upgrade to PHP version 5.2.9 or above, http://www.php.net/downloads.php Workaround: For workaround refer below link, http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15 References: http://www.php.net/releases/5_2_9.php http://www.openwall.com/lists/oss-security/2009/04/01/9 CVSS Score: CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:N/I:N/A:P) CVSS Temporal Score : 3.7 Risk factor : Medium CVE : CVE-2009-1272 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800393
Warning	http (80/tcp)	Overview: The host is running PHP and is prone to Cross-Site Scripting vulnerability. Vulnerability Insight: The flaw is caused due to improper handling of certain inputs when display_errors settings is enabled. Impact: Successful exploitation could allow attackers to inject arbitrary web script or HTML via unspecified vectors and conduct Cross-Site Scripting attacks. Impact Level: Application Affected Software/OS: PHP, PHP version 5.2.7 and prior on all running platform. Fix: Upgrade to version 5.2.8 or later http://www.php.net/downloads.php References: http://jvn.jp/en/jp/JVN50327700/index.html http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html CVSS Score: CVSS Base Score : 2.6 (AV:N/AC:H/Au:NR/C:N/I:P/A:N) CVSS Temporal Score : 1.9 Risk factor : Low CVE : CVE-2008-5814 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800334
Warning	http (80/tcp)	Overview : The host is running Apache, which is prone to cross-site scripting vulnerability. Vulnerability Insight : Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user. Impact : Remote attackers can execute arbitrary script code. Impact Level : Application Affected Software/OS : Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9 on All Platform *** Note: The script might report a False Positive as it is only checking for the vulnerable version of Apache. Vulnerability is only when mod_proxy and mod_proxy_ftp is configured with the installed Apache version. ***

Fix : Fixed is available in the SVN repository,
http://svn.apache.org/viewvc?view=rev&revision=682871
http://svn.apache.org/viewvc?view=rev&revision=682868

References :
http://httpd.apache.org/
http://www.securityfocus.com/archive/1/495180
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score :
CVSS Base Score : 5.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 4.5
Risk factor : Medium
CVE : CVE-2008-2939
BID : 30560
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900107

Warning	http (80/tcp)	Overview: PHP is prone to multiple security vulnerabilities. Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported. These issues affect PHP 5.2.8 and prior versions. Solution: The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information. See also: http://www.securityfocus.com/bid/33927 Risk factor : Medium CVE : CVE-2009-1271 BID : 33927 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100146
Warning	http (80/tcp)	Overview: Apache HTTP server is prone to a security-bypass vulnerability related to the handling of specific configuration directives. A local attacker may exploit this issue to execute arbitrary code within the context of the webserver process. This may result in elevated privileges or aid in further attacks. Versions prior to Apache 2.2.9 are vulnerable. Solution: Updates are available. Please see http://httpd.apache.org/ for more Information. See also: http://www.securityfocus.com/bid/35115 Risk factor: Medium CVE : CVE-2009-1195 BID : 35115 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100211
Warning	http (80/tcp)	Overview: The host is installed with WordPress and is prone to Cross Site Request Forgery(CSRF) Vulnerabilities. Vulnerability Insight: The flaw is caused due to incorrect usage of _REQUEST super global array, which leads to cross site request forgery (CSRF) attacks via crafted cookies. Impact: Successful attack could lead to execution of arbitrary script code and can cause denial of service condition. Impact Level: Application Affected Software/OS: WordPress 2.6.3 and earlier on all running platforms. Fix: No solution/patch is available as on 21st November, 2008. Information regarding this issue will updated once the solution details are available. For updates refer, http://wordpress.org/

NOTE: This issue relies on the presence of an independent vulnerability that allows cookie injection.

References:
http://openwall.com/lists/oss-security/2008/11/14/1
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=504771

CVSS Score:
CVSS Base Score : 4.0 (AV:N/AC:H/Au:NR/C:N/I:P/A:P)
CVSS Temporal Score : 3.6
Risk factor: Medium
CVE : CVE-2008-5113
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800140

Warning http (80/tcp)

Overview: This host is running Apache Web Server and is prone to Information Disclosure Vulnerability.

Vulnerability Insight:
This flaw is caused due to an error in 'mod_proxy_ajp' when handling improperly malformed POST requests.

Impact:
Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

Workaround:
Update mod_proxy_ajp.c through SVN Repository (Revision 767089)
http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Fix: No solution or patch is available as on 29th April, 2009. Information regarding this issue will be updated once the solution details are available. For further updates refer, http://httpd.apache.org/download.cgi

References:
http://secunia.com/advisories/34827
http://xforce.iss.net/xforce/xfdb/50059
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 4.0
Risk factor: Medium
CVE : CVE-2009-1191
BID : 34663
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900499

Warning http (80/tcp)

Overview: The host is running PHP and is prone to Memory Information Disclosure vulnerability.

Vulnerability Insight:
The flaw is caused due to improper validation of bgd_color or clrBack argument in imageRotate function.

Impact:
Successful exploitation could let the attacker read the contents of arbitrary memory locations through a crafted value for an indexed image.

Impact Level: Application

Affected Software/OS:
PHP version 5.x to 5.2.8 on all running platform.

Fix: No solution or patch is available as on 31st December, 2008. Information regarding this issue will be updated once the solution details are available. For updates refer, http://www.php.net/

References:
http://securitytracker.com/alerts/2008/Dec/1021494.html
http://downloads.securityfocus.com/vulnerabilities/exploits/33002.php
http://downloads.securityfocus.com/vulnerabilities/exploits/33002-2.php

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 2.9
Risk factor: Low
CVE : CVE-2008-5498
BID : 33002
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900186

Informational http (80/tcp)
A web server is running on this port
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330

Informational http (80/tcp)
The remote web server type is :

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107

Informational http (80/tcp)
Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to
cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when
used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give
him their credentials.

Solution :

Disable these methods.

See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Plugin output :

Solution :
Add the following lines for each virtual host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

CVE : CVE-2004-2320
BID : 9506, 9561, 11604
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11213

Informational http (80/tcp)
The following directories were discovered:
/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
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11032

Informational https (443/tcp)
Synopsis :

An SSL detection issue might impede the OpenVAS Scan.

Description :

		OpenVAS has discovered that it is talking in plain HTTP on a SSL port. OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped. Solution : Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port. Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.15588
Informational	ntp-gps-data (12321/tcp)	A web server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ntp-gps-data (12321/tcp)	Synopsis : An SSL detection issue might impede the OpenVAS Scan. Description : OpenVAS has discovered that it is talking in plain HTTP on a SSL port. OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped. Solution : Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port. Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.15588
Informational	ntp-gps-data (12321/tcp)	Synopsis : Remote web server does not reply with 404 error code. Description : This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead. OpenVAS enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10386
Informational	ntp-gps-data (12321/tcp)	The remote web server type is : MiniServ/0.01 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107
Warning	ssh (22/tcp)	Overview: The host is installed with OpenSSH and is prone to information disclosure vulnerability. Vulnerability Insight: The flaw is caused due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode. Impact: Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session.

		Impact Level: Application Affected Software/OS: Versions prior to OpenSSH 5.2 are vulnerable. Various versions of SSH Tectia are also affected. Fix: Upgrade to higher version http://www.openssh.com/portable.html References: http://www.securityfocus.com/bid/32319 Risk factor: Medium BID : 32319 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100153
Informational	ssh (22/tcp)	An ssh server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ssh (22/tcp)	No key given for SLAD checks. SLAD checks will be disabled. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90002
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1.2 Remote SSH supported authentication : publickey,password OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10267
Informational	ssh (22/tcp)	No key given for SLAD checks. SLAD checks will be disabled. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90003
Informational	ntp (123/udp)	A NTP (Network Time Protocol) server is listening on this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10884
Informational	general/tcp	ICMP based OS fingerprint results: Linux Kernel 2.6.11 (accuracy 100%) Linux Kernel 2.6.10 (accuracy 100%) Linux Kernel 2.6.9 (accuracy 100%) Linux Kernel 2.6.8 (accuracy 100%) Linux Kernel 2.6.7 (accuracy 100%) Linux Kernel 2.6.6 (accuracy 100%) Linux Kernel 2.6.5 (accuracy 100%) Linux Kernel 2.6.4 (accuracy 100%) Linux Kernel 2.6.3 (accuracy 100%) Linux Kernel 2.6.2 (accuracy 100%) Linux Kernel 2.6.1 (accuracy 100%) Linux Kernel 2.6.0 (accuracy 100%) Linux Kernel 2.4.30 (accuracy 100%) Linux Kernel 2.4.29 (accuracy 100%) Linux Kernel 2.4.28 (accuracy 100%) Linux Kernel 2.4.27 (accuracy 100%) Linux Kernel 2.4.26 (accuracy 100%) Linux Kernel 2.4.25 (accuracy 100%) Linux Kernel 2.4.24 (accuracy 100%) Linux Kernel 2.4.23 (accuracy 100%) Linux Kernel 2.4.22 (accuracy 100%) Linux Kernel 2.4.21 (accuracy 100%) Linux Kernel 2.4.20 (accuracy 100%) Linux Kernel 2.4.19 (accuracy 100%) Linux Kernel 2.0.36 (accuracy 100%) Linux Kernel 2.0.34 (accuracy 100%) Linux Kernel 2.0.30 (accuracy 100%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002
Informational	general/tcp	Nikto could not be found in your system path. OpenVAS was unable to execute Nikto and to perform the scan you requested. Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.14260
Informational	general/tcp	Synopsis : The remote service implements TCP timestamps. 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 sometimes be computed. See also : http://www.ietf.org/rfc/rfc1323.txt Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.80091
Informational	general/tcp	Information about this scan : OpenVAS version : 2.0.1 Plugin feed version : 200906251300 Type of plugin feed : OpenVAS NVT Feed Scanner IP : 192.168.1.106 Port scanner(s) : openvas_tcp_scanner Port range : default Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Max hosts : 20 Max checks : 4 Scan duration : unknown (ping_host.nasl not launched?) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.114	sunrpc (111/tcp)	Security note(s) found
192.168.1.114	submission (587/tcp)	Security warning(s) found
192.168.1.114	ssh (22/tcp)	Security note(s) found
192.168.1.114	smtp (25/tcp)	Security warning(s) found
192.168.1.114	general/SMBClient	No Information
192.168.1.114	sunrpc (111/udp)	Security note(s) found
192.168.1.114	general/tcp	Security note(s) found
192.168.1.114	router (520/udp)	Security note(s) found

Security Issues and Fixes: 192.168.1.114

Type	Port	Issue and Fix
Informational	sunrpc (111/tcp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11111
Warning	submission (587/tcp)	Overview: The Mailserver on this host answers to VRFY and/or EXPN requests. VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc. OpenVAS suggests that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP. Solution: Disable VRFY and EXPN on your Mailserver.

		Risk factor : Medium OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100072
Informational	submission (587/tcp)	An SMTP server is running on this port Here is its banner : 220 opensolaris-vm.local ESMTP Sendmail 8.14.2+Sun/8.14.2; Wed, 1 Jul 2009 19:42:00 -0700 (PDT) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	submission (587/tcp)	Remote SMTP server banner : 220 opensolaris-vm.local ESMTP Sendmail 8.14.2+Sun/8.14.2; Wed, 1 Jul 2009 19:42:19 -0700 (PDT) This is probably: Sendmail version 8.14.2+Sun OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10263
Informational	ssh (22/tcp)	An ssh server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ssh (22/tcp)	No key given for SLAD checks. SLAD checks will be disabled. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90002
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-Sun_SSH_1.2 Remote SSH supported authentication : gssapi-keyex,gssapi-with-mic,publickey,password,keyboard-interactive OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10267
Informational	ssh (22/tcp)	No key given for SLAD checks. SLAD checks will be disabled. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90003
Warning	smtp (25/tcp)	Overview: The Mailserver on this host answers to VRFY and/or EXPN requests. VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc. OpenVAS suggests that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP. Solution: Disable VRFY and EXPN on your Mailserver. Risk factor : Medium OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100072
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 opensolaris-vm.local ESMTP Sendmail 8.14.2+Sun/8.14.2; Wed, 1 Jul 2009 19:42:02 -0700 (PDT) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 opensolaris-vm.local ESMTP Sendmail 8.14.2+Sun/8.14.2; Wed, 1 Jul 2009 19:42:19 -0700 (PDT) This is probably: Sendmail version 8.14.2+Sun OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10263
Informational	sunrpc (111/udp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11111
Informational	general/tcp	ICMP based OS fingerprint results: HP UX 11.0 (accuracy 95%) Sun Solaris 10 (SunOS 5.10) (accuracy 95%) OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002
Informational	general/tcp	Information about this scan : OpenVAS version : 2.0.1

Plugin feed version : 200906251300
Type of plugin feed : OpenVAS NVT Feed
Scanner IP : 192.168.1.106
Port scanner(s) : openvas_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Max hosts : 20
Max checks : 4
Scan duration : unknown (ping_host.nasl not launched?)

OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506

Informational	router (520/udp)	A RIP-2 agent is running on this port. Risk factor: None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11822

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.115	ssh (22/tcp)	Security warning(s) found
192.168.1.115	http (80/tcp)	Security hole(s) found
192.168.1.115	https (443/tcp)	Security note(s) found
192.168.1.115	ntp-gps-data (12321/tcp)	Security note(s) found
192.168.1.115	ntp (123/udp)	Security note(s) found
192.168.1.115	general/SMBClient	No Information
192.168.1.115	general/tcp	Security hole(s) found

Security Issues and Fixes: 192.168.1.115

Type	Port	Issue and Fix
Warning	ssh (22/tcp)	Overview: The host is installed with OpenSSH and is prone to information disclosure vulnerability. Vulnerability Insight: The flaw is caused due to the improper handling of errors within an SSH session encrypted with a block cipher algorithm in the Cipher-Block Chaining 'CBC' mode. Impact: Successful exploits will allow attackers to obtain four bytes of plaintext from an encrypted session. Impact Level: Application Affected Software/OS: Versions prior to OpenSSH 5.2 are vulnerable. Various versions of SSH Tectia are also affected. Fix: Upgrade to higher version http://www.openssh.com/portable.html References: http://www.securityfocus.com/bid/32319 Risk factor: Medium BID : 32319 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100153
Informational	ssh (22/tcp)	An ssh server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ssh (22/tcp)	No key given for SLAD checks. SLAD checks will be disabled. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90002
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1.2 Remote SSH supported authentication : publickey,password

OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10267

Informational ssh (22/tcp)
No key given for SLAD checks. SLAD checks will be disabled.
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.90003

Vulnerability http (80/tcp)

Overview: The host is installed with PHP, that is prone to multiple vulnerabilities.

Vulnerability Insight:
The flaws are caused by,
- an unspecified stack overflow error in FastCGI SAPI (fastcgi.c).
- an error during path translation in cgi_main.c.
- an error with an unknown impact/attack vectors.
- an unspecified error within the processing of incomplete multibyte characters in escapeshellcmd() API function.
- error in curl/interface.c in the cURL library(libcurl), which could be exploited by attackers to bypass safe_mode security restrictions.
- an error in PCRE. i.e buffer overflow error when handling a character class containing a very large number of characters with codepoints greater than 255(UTF-8 mode).

Impact:
Successful exploitation could result in remote arbitrary code execution, security restrictions bypass, access to restricted files, denial of service.

Impact Level: System

Affected Software/OS:
PHP version prior to 5.2.6

Fix:
Upgrade to PHP version 5.2.6 or above,
http://www.php.net/downloads.php

References:
http://pcre.org/changelog.txt
http://www.php.net/ChangeLog-5.php
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0176
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0178
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086

CVSS Score:
CVSS Base Score : 9.0 (AV:N/AC:L/Au:NR/C:P/I:P/A:C)
CVSS Temporal Score : 7.0
Risk factor : High
CVE : CVE-2008-2050, CVE-2008-2051, CVE-2007-4850, CVE-2008-0599, CVE-2008-0674
BID : 29009, 27413, 27786
Other references : CB-A:08-0118
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800110

Vulnerability http (80/tcp)

Overview: The host is running PHP and is prone to Buffer Overflow vulnerability.

Vulnerability Insight:
The flaw is caused due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions.

Impact:
Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity.

Impact Level: Application

Affected Software/OS:
PHP version 4.3.0 to 5.2.6 on all running platform.

Fix: Upgrade to version 5.2.7 or later,
http://www.php.net/downloads.php

References:
http://bugs.php.net/bug.php?id=45722
http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0477.html

CVSS Score:

CVSS Base Score : 10.0 (AV:N/AC:L/Au:NR/C:C/I:C/A:C)
CVSS Temporal Score : 7.4
Risk factor: High
CVE : CVE-2008-5557
BID : 32948
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900185

Vulnerability http (80/tcp)

Overview:
The host is running PHP and is prone to denial of service vulnerability.

Vulnerability Insight:
This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server.

Impact:
Successful exploitation will let the local attackers to crash an affected web server.

Impact Level: Application

Affected Software/OS:
PHP version 4.4.4 and prior
PHP 5.1.x to 5.1.6
PHP 5.2.x to 5.2.5

Fix: No solution or patch is available as on 17th March, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, http://www.php.net

References:
http://bugs.php.net/bug.php?id=27421
https://bugzilla.redhat.com/show_bug.cgi?id=479272

CVSS Score:
CVSS Base Score : 2.1 (AV:L/AC:L/Au:NR/C:N/I:P/A:N)
CVSS Temporal Score : 1.9
Risk factor : Low
CVE : CVE-2009-0754
BID : 33542
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800373

Vulnerability http (80/tcp)

Overview: The host is running PHP and is prone to Security Bypass and File Writing vulnerability.

Vulnerability Insight:
The flaw is caused due to,
- An error in initialization of 'page_uid' and 'page_gid' global variables for use by the SAPI 'php_getuid' function, which bypass the safe_mode restrictions.
- When 'safe_mode' is enabled through a 'php_admin_flag' setting in 'httpd.conf' file, which does not enforce the 'error_log', 'safe_mode restrictions.
- In 'ZipArchive::extractTo' function which allows attacker to write files via a ZIP file.

Impact:
Successful exploitation could allow remote attackers to write arbitrary file, bypass security restrictions and cause directory traversal attacks.

Impact Level: System/Application

Affected Software/OS:
PHP versions prior to 5.2.7.

Fix: Upgrade to version 5.2.7 or later
http://www.php.net/downloads.php

References:
http://www.php.net/ChangeLog-5.php#5.2.7
http://www.php.net/archive/2008.php#id2008-12-07-1
http://www.securityfocus.com/archive/1/archive/1/498985/100/0/threaded

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 5.9

Risk factor: High
CVE : CVE-2008-5624, CVE-2008-5625, CVE-2008-5658
BID : 32383, 32625, 32688
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900184

Warning http (80/tcp)

Overview: The host is installed with PHP and is prone to Denial of Service vulnerability.

Vulnerability Insight:
Improper handling of .zip file while doing extraction via php_zip_make_relative_path function in php_zip.c file.

Impact:
Successful exploitation could result in denial of service condition.

Impact Level: Application

Affected Software/OS:
PHP version prior to 5.2.9

Fix:
Upgrade to PHP version 5.2.9 or above,
http://www.php.net/downloads.php

Workaround:
For workaround refer below link,
http://cvs.php.net/viewvc.cgi/php-src/ext/json/JSON_parser.c?r1=1.1.2.14&r2=1.1.2.15

References:
http://www.php.net/releases/5_2_9.php
http://www.openwall.com/lists/oss-security/2009/04/01/9

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.7
Risk factor : Medium
CVE : CVE-2009-1272
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800393

Warning http (80/tcp)

Overview: The host is running PHP and is prone to Cross-Site Scripting vulnerability.

Vulnerability Insight:
The flaw is caused due to improper handling of certain inputs when display_errors settings is enabled.

Impact:
Successful exploitation could allow attackers to inject arbitrary web script or HTML via unspecified vectors and conduct Cross-Site Scripting attacks.

Impact Level: Application

Affected Software/OS:
PHP, PHP version 5.2.7 and prior on all running platform.

Fix: Upgrade to version 5.2.8 or later
http://www.php.net/downloads.php

References:
http://jvn.jp/en/jp/JVN50327700/index.html
http://jvndb.jvn.jp/en/contents/2008/JVNDB-2008-000084.html

CVSS Score:
CVSS Base Score : 2.6 (AV:N/AC:H/Au:NR/C:N/I:P/A:N)
CVSS Temporal Score : 1.9
Risk factor : Low
CVE : CVE-2008-5814
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800334

Warning http (80/tcp)

Overview : The host is running Apache, which is prone to cross-site scripting vulnerability.

Vulnerability Insight :

Input passed to the module mod_proxy_ftp with wildcard character is not properly sanitized before returning to the user.

Impact : Remote attackers can execute arbitrary script code.

Impact Level : Application

Affected Software/OS :
Apache 2.0.0 to 2.0.63 and Apache 2.2.0 to 2.2.9 on All Platform

***
Note: The script might report a False Positive as it is only checking for the vulnerable version of Apache. Vulnerability is only when mod_proxy and mod_proxy_ftp is configured with the installed Apache version.
***

Fix : Fixed is available in the SVN repository,
http://svn.apache.org/viewvc?view=rev&revision=682871
http://svn.apache.org/viewvc?view=rev&revision=682868

References :
http://httpd.apache.org/
http://www.securityfocus.com/archive/1/495180
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score :
CVSS Base Score : 5.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 4.5
Risk factor : Medium
CVE : CVE-2008-2939
BID : 30560
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900107

Warning	http (80/tcp)	Overview: PHP is prone to multiple security vulnerabilities. Successful exploits could allow an attacker to cause a denial-of-service condition. An unspecified issue with an unknown impact was also reported. These issues affect PHP 5.2.8 and prior versions. Solution: The vendor has released PHP 5.2.9 to address these issues. Please see http://www.php.net/ fore more information. See also: http://www.securityfocus.com/bid/33927 Risk factor : Medium CVE : CVE-2009-1271 BID : 33927 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100146
Warning	http (80/tcp)	Overview: Apache HTTP server is prone to a security-bypass vulnerability related to the handling of specific configuration directives. A local attacker may exploit this issue to execute arbitrary code within the context of the webserver process. This may result in elevated privileges or aid in further attacks. Versions prior to Apache 2.2.9 are vulnerable. Solution: Updates are available. Please see http://httpd.apache.org/ for more Information. See also: http://www.securityfocus.com/bid/35115 Risk factor: Medium CVE : CVE-2009-1195 BID : 35115 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100211
Warning	http (80/tcp)	Overview: This host is running Apache Web Server and is prone to Information Disclosure Vulnerability. Vulnerability Insight:

This flaw is caused due to an error in 'mod_proxy_ajp' when handling improperly malformed POST requests.

Impact:
Successful exploitation will let the attacker craft a special HTTP POST request and gain sensitive information about the web server.

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

Workaround:
Update mod_proxy_ajp.c through SVN Repository (Revision 767089)
http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

Fix: No solution or patch is available as on 29th April, 2009. Information regarding this issue will be updated once the solution details are available. For further updates refer, http://httpd.apache.org/download.cgi

References:
http://secunia.com/advisories/34827
http://xforce.iss.net/xforce/xfdb/50059
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 4.0
Risk factor: Medium
CVE : CVE-2009-1191
BID : 34663
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900499

Warning	http (80/tcp)	Overview: The host is running PHP and is prone to Memory Information Disclosure vulnerability. Vulnerability Insight: The flaw is caused due to improper validation of bgd_color or clrBack argument in imageRotate function. Impact: Successful exploitation could let the attacker read the contents of arbitrary memory locations through a crafted value for an indexed image. Impact Level: Application Affected Software/OS: PHP version 5.x to 5.2.8 on all running platform. Fix: No solution or patch is available as on 31st December, 2008. Information regarding this issue will be updated once the solution details are available. For updates refer, http://www.php.net/ References: http://securitytracker.com/alerts/2008/Dec/1021494.html http://downloads.securityfocus.com/vulnerabilities/exploits/33002.php http://downloads.securityfocus.com/vulnerabilities/exploits/33002-2.php CVSS Score: CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N) CVSS Temporal Score : 2.9 Risk factor: Low CVE : CVE-2008-5498 BID : 33002 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.900186
Warning	http (80/tcp)	Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc. Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.

The file 'robots.txt' contains the following:
$Id: robots.txt,v 1.7.2.3 2008/12/10 20:24:38 drumm Exp $
#
robots.txt
#
This file is to prevent the crawling and indexing of certain parts
of your site by web crawlers and spiders run by sites like Yahoo!
and Google. By telling these "robots" where not to go on your site,
you save bandwidth and server resources.
#
This file will be ignored unless it is at the root of your host:
Used: http://example.com/robots.txt
Ignored: http://example.com/site/robots.txt
#
For more information about the robots.txt standard, see:
http://www.robotstxt.org/wc/robots.html
#
For syntax checking, see:
http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /sites/
Disallow: /themes/
Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /contact/
Disallow: /logout/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=contact/
Disallow: /?q=logout/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/

Risk factor : Medium
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10302

Informational	http (80/tcp)	A web server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	http (80/tcp)	The remote web server type is : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107

Informational http (80/tcp)

Overview:
This host is running Drupal, an open source content management platform.

See also:
http://drupal.org/

Risk factor : None

Drupal Version 'unknown' was detected on the remote host in the following directory(s):

/

OpenVAS ID : 1.3.6.1.4.1.25623.1.0.100169

Informational http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to
cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when
used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give
him their credentials.

Solution :

Disable these methods.

See also :

http://www.kb.cert.org/vuls/id/867593

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Plugin output :

Solution :
Add the following lines for each virtual host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

CVE : CVE-2004-2320
BID : 9506, 9561, 11604
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.11213

Informational https (443/tcp)

Synopsis :

An SSL detection issue might impede the OpenVAS Scan.

Description :

OpenVAS has discovered that it is talking in plain HTTP on a SSL port.

OpenVAS has corrected this issue by enabled HTTPS on this port only. However
if other SSL ports are used on the remote host, they might be skipped.

Solution :

Enable SSL tests in the 'Services' preference setting, or increase the
timeouts if this option is already set and the plugin missed
this port.

		Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.15588
Informational	ntp-gps-data (12321/tcp)	A web server is running on this port OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10330
Informational	ntp-gps-data (12321/tcp)	Synopsis : An SSL detection issue might impede the OpenVAS Scan. Description : OpenVAS has discovered that it is talking in plain HTTP on a SSL port. OpenVAS has corrected this issue by enabled HTTPS on this port only. However if other SSL ports are used on the remote host, they might be skipped. Solution : Enable SSL tests in the 'Services' preference setting, or increase the timeouts if this option is already set and the plugin missed this port. Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.15588
Informational	ntp-gps-data (12321/tcp)	Synopsis : Remote web server does not reply with 404 error code. Description : This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead. OpenVAS enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate Risk factor : None OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10386
Informational	ntp-gps-data (12321/tcp)	The remote web server type is : MiniServ/0.01 OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10107
Informational	ntp (123/udp)	A NTP (Network Time Protocol) server is listening on this port. Risk factor : Low OpenVAS ID : 1.3.6.1.4.1.25623.1.0.10884
Vulnerability	general/tcp	Overview: This host is installed with Drupal and is prone to Multiple Vulnerabilities. Vulnerability Insight: Flaws are due to, - ability to view attached file content which they don't have access. - deficiency in the user module allows users who had been blocked by access rules. - weakness in the node module API allows for node validation to be bypassed in certain circumstances. Impact: Successful exploitation allows authenticated users to bypass access restrictions and can even allows unauthorized users to obtain sensitive information. Impact Level: Application Affected Software/OS:

Drupal Version 5.x prior to 5.11 and 6.x prior to 6.5 on all running platform.

Fix: Upgrade Drupal Version 5.x to 5.11/6.x to Drupal 6.5 or later.
http://drupal.org/

References:
http://drupal.org/node/318706

CVSS Score:
CVSS Base Score : 6.0 (AV:N/AC:M/Au:SI/C:P/I:P/A:P)
CVSS Temporal Score : 4.4
Risk factor: Medium
CVE : CVE-2008-4789, CVE-2008-4790, CVE-2008-4791, CVE-2008-4793
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.800123

Informational general/tcp ICMP based OS fingerprint results:

Linux Kernel 2.6.11 (accuracy 100%)
Linux Kernel 2.6.10 (accuracy 100%)
Linux Kernel 2.6.9 (accuracy 100%)
Linux Kernel 2.6.8 (accuracy 100%)
Linux Kernel 2.6.7 (accuracy 100%)
Linux Kernel 2.6.6 (accuracy 100%)
Linux Kernel 2.6.5 (accuracy 100%)
Linux Kernel 2.6.4 (accuracy 100%)
Linux Kernel 2.6.3 (accuracy 100%)
Linux Kernel 2.6.2 (accuracy 100%)
Linux Kernel 2.6.1 (accuracy 100%)
Linux Kernel 2.6.0 (accuracy 100%)
Linux Kernel 2.4.30 (accuracy 100%)
Linux Kernel 2.4.29 (accuracy 100%)
Linux Kernel 2.4.28 (accuracy 100%)
Linux Kernel 2.4.27 (accuracy 100%)
Linux Kernel 2.4.26 (accuracy 100%)
Linux Kernel 2.4.25 (accuracy 100%)
Linux Kernel 2.4.24 (accuracy 100%)
Linux Kernel 2.4.23 (accuracy 100%)
Linux Kernel 2.4.22 (accuracy 100%)
Linux Kernel 2.4.21 (accuracy 100%)
Linux Kernel 2.4.20 (accuracy 100%)
Linux Kernel 2.4.19 (accuracy 100%)
Linux Kernel 2.0.36 (accuracy 100%)
Linux Kernel 2.0.34 (accuracy 100%)
Linux Kernel 2.0.30 (accuracy 100%)

OpenVAS ID : 1.3.6.1.4.1.25623.1.0.102002

Informational general/tcp Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment.
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.14260

Informational general/tcp

Synopsis :

The remote service implements TCP timestamps.

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 sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Risk factor :

None
OpenVAS ID : 1.3.6.1.4.1.25623.1.0.80091

Informational general/tcp Information about this scan :

OpenVAS version : 2.0.1
Plugin feed version : 200906251300
Type of plugin feed : OpenVAS NVT Feed
Scanner IP : 192.168.1.106
Port scanner(s) : openvas_tcp_scanner
Port range : default

Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Max hosts : 20
Max checks : 4
Scan duration : unknown (ping_host.nasl not launched?)

OpenVAS ID : 1.3.6.1.4.1.25623.1.0.19506

This file was generated by the OpenVAS security scanner.