Nessus Report

Nessus Scan Report

Wed, 01 Jun 2016 21:12:22 WEST

Table Of Contents

Vulnerabilities By Host

[-] Collapse All
[+] Expand All

192.168.15.120

Scan Information

Start time:	Wed Jun 1 21:07:33 2016
End time:	Wed Jun 1 21:12:20 2016

Host Information

Netbios Name:	PC-VITTIMA
IP:	192.168.15.120
MAC Address:	08:00:27:b8:40:cd
OS:	Microsoft Windows XP, Microsoft Windows XP Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
27	45	79	1	70	222

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

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 that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

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

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

The ICMP timestamps seem to be in little endian format (not in network format)
The remote clock is synchronized with the local clock.

0/tcp

73182 - Microsoft Windows XP Unsupported Installation Detection [-/+]

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

http://www.nessus.org/u?33ca6af0

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2014/03/25, Modification date: 2015/10/21

Ports

tcp/0

57608 - SMB Signing Disabled [-/+]

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Publication date: 2012/01/19, Modification date: 2016/01/13

Ports

tcp/0

24786 - Nessus Windows Scan Not Performed with Admin Privileges [-/+]

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

It was not possible to connect to '\\PC-VITTIMA\ADMIN$' with the supplied credentials.

25220 - TCP/IP Timestamps Supported [-/+]

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection [-/+]

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

http://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

The following card manufacturers were identified :

08:00:27:b8:40:cd : Cadmus Computer Systems

11936 - OS Identification [-/+]

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2016/02/24

Ports

tcp/0

Remote operating system : Microsoft Windows XP
Microsoft Windows XP Service Pack 1
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to os-signatures@nessus.org. Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

HTTP:Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
NTP:!:unknown
SinFP:
P1:B11113:F0x12:W64240:O0204ffff:M1460:
P2:B11113:F0x12:W64240:O0204ffff010303000101080a00000
000000000001010402:M1460:
P3:B11021:F0x04:W0:O0:M0
P4:6700_7_p=135
SMTP:!:220 pc-vittima SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
SSLcert:!:i/CN:localhosts/CN:localhost
e48bdd0816e96dbe014c4c9d51632c93f776a486

The remote host is running one of these operating systems :
Microsoft Windows XP
Microsoft Windows XP Service Pack 1

45590 - Common Platform Enumeration (CPE) [-/+]

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/cpe.cfm

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Ports

tcp/0

The remote operating system matched the following CPE's :

cpe:/o:microsoft:windows_xp
cpe:/o:microsoft:windows_xp::sp1 -> Microsoft Windows XP Service Pack 1

Following application CPE's matched on the remote system :

cpe:/a:openssl:openssl:0.9.8k -> OpenSSL Project OpenSSL 0.9.8k
cpe:/a:modssl:mod_ssl:2.2.12
cpe:/a:apache:http_server:2.2.12 -> Apache Software Foundation Apache HTTP Server 2.2.12
cpe:/a:apache:mod_perl:2.0.4
cpe:/a:php:php:5.3.0 -> PHP 5.3.0

54615 - Device Type [-/+]

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

Remote device type : general-purpose
Confidence level : 99

66334 - Patch Report [-/+]

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Publication date: 2013/07/08, Modification date: 2016/05/10

Ports

tcp/0

. You need to take the following 5 actions :

[Apache 2.2.x < 2.2.28 Multiple Vulnerabilities (77531)]

+ Action to take : Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

+Impact : Taking this action will resolve 35 different vulnerabilities (CVEs).

[MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280) (uncredentialed check) (21696)]

+ Action to take : Microsoft has released a set of patches for Windows 2000, XP and 2003.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution

(2508429) (remote check) (53503)]

+ Action to take : Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS (87219)]

+ Action to take : Upgrade to OpenSSL version 0.9.8zh or later.

+Impact : Taking this action will resolve 47 different vulnerabilities (CVEs).

[PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (77285)]

+ Action to take : Upgrade to PHP version 5.3.29 or later.

+Impact : Taking this action will resolve 97 different vulnerabilities (CVEs).

19506 - Nessus Scan Information [-/+]

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2016/04/08

Ports

tcp/0

Information about this scan :

Nessus version : 6.7.0
Plugin feed version : 201606010530
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : SCAN WINDOWS XP
Scanner IP : 192.168.15.101
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/6/1 21:07 WEST
Scan duration : 287 sec

0/udp

10287 - Traceroute Information [-/+]

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports

udp/0

For your information, here is the traceroute from 192.168.15.101 to 192.168.15.120
:
192.168.15.101
192.168.15.120

21/tcp

10081 - FTP Privileged Port Bounce Scan [-/+]

Synopsis

The remote FTP server is vulnerable to a FTP server bounce attack.

Description

It is possible to force the remote FTP server to connect to third parties using the PORT command.

The problem allows intruders to use your network resources to scan other hosts,

making them think the attack comes from your network.

See Also

http://archives.neohapsis.com/archives/bugtraq/1995_3/0047.html

Solution

See the CERT advisory in the references for solutions and workarounds.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.1 (CVSS2#E:F/RL:U/RC:ND)

References

BID	126
CVE	CVE-1999-0017
XREF	OSVDB:71
XREF	OSVDB:87439
XREF	OSVDB:88560
XREF	OSVDB:88561
XREF	OSVDB:88562
XREF	OSVDB:88563
XREF	OSVDB:88564
XREF	OSVDB:88565
XREF	OSVDB:88566
XREF	OSVDB:88567
XREF	OSVDB:88568
XREF	OSVDB:88569
XREF	OSVDB:88570
XREF	OSVDB:88571
XREF	OSVDB:88572
XREF	CERT-CC:CA-1997-27

Plugin Information:

Publication date: 1999/06/22, Modification date: 2016/05/05

Ports

tcp/21

The following command, telling the server to connect to 169.254.31.162 on port 10794:

PORT 169,254,31,162,42,42

produced the following output:

200 Port command successful

10079 - Anonymous FTP Enabled [-/+]

Synopsis

Anonymous logins are allowed on the remote FTP server.

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials.
This allows a user to access any files made available on the FTP server.

Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0497
XREF	OSVDB:69

Plugin Information:

Publication date: 1999/06/22, Modification date: 2014/04/02

Ports

tcp/21

The contents of the remote FTP root are :
drwxr-xr-x 1 ftp ftp 0 Aug 06 2009 incoming
-r--r--r-- 1 ftp ftp 187 Aug 06 2009 onefile.html

34324 - FTP Supports Cleartext Authentication [-/+]

Synopsis

Authentication credentials might be intercepted.

Description

The remote FTP server allows the user's name and password to be transmitted in cleartext, which could be intercepted by a network sniffer or a man-in-the-middle attack.

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522

XREF	CWE:523
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2008/10/01, Modification date: 2015/06/23

Ports

tcp/21

This FTP server does not support 'AUTH TLS'.

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/21

Port 21/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/21

An FTP server is running on this port.

10092 - FTP Server Detection [-/+]

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/05/04

Ports

tcp/21

The remote FTP banner is :

220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/

25/tcp

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/25

Port 25/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/25

An SMTP server is running on this port.

10263 - SMTP Server Detection [-/+]

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/25

Remote SMTP server banner :

220 pc-vittima SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here

69/udp

11819 - TFTP Daemon Detection [-/+]

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 2003/08/13, Modification date: 2016/02/22

Ports

udp/69

80/tcp

58987 - PHP Unsupported Version Detection [-/+]

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2012/05/04, Modification date: 2015/10/06

Ports

tcp/80

Source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
End of support date : 2014/08/14
Announcement : http://php.net/archive/2014.php#id2014-08-14-1
Supported versions : 5.6.x / 5.5.x

60085 - PHP 5.3.x < 5.3.15 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.15, and is, therefore, potentially affected by the following vulnerabilities :

- An unspecified overflow vulnerability exists in the function '_php_stream_scandir' in the file 'main/streams/streams.c'. (CVE-2012-2688)

- An unspecified error exists that can allow the 'open_basedir' constraint to be bypassed.
(CVE-2012-3365)

See Also

http://www.php.net/ChangeLog-5.php#5.3.15

Solution

Upgrade to PHP version 5.3.15 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	54612
BID	54638
CVE	CVE-2012-2688
CVE	CVE-2012-3365
XREF	OSVDB:84100
XREF	OSVDB:84126

Plugin Information:

Publication date: 2012/07/20, Modification date: 2013/10/23

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.15

78555 - OpenSSL Unsupported [-/+]

Synopsis

The remote service is not a supported version.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html
http://www.nessus.org/u?4d55548d

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2014/10/17, Modification date: 2016/01/06

Ports

tcp/80

Installed version : 0.9.8k
Supported versions : 1.0.2 / 1.0.1

45004 - Apache 2.2.x < 2.2.15 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :

- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)

- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)

- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)

- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)

- Added 'mod_reqtimeout' module to mitigate Slowloris attacks. (CVE-2007-6750)

See Also

http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
https://archive.apache.org/dist/httpd/CHANGES_2.2.15

Solution

Upgrade to Apache version 2.2.15 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	21865
BID	36935
BID	38491
BID	38494
BID	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XREF	OSVDB:59969
XREF	OSVDB:62674
XREF	OSVDB:62675
XREF	OSVDB:62676
XREF	Secunia:38776
XREF	CWE:200

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2010/10/20, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.15

57603 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow [-/+]

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

According to its self-reported banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr_palloc()' that could cause a heap overflow.

Note that the Apache HTTP server itself does not pass unsanitized, user-provided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache 2.2.13 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	35949
CVE	CVE-2009-2412
XREF	OSVDB:56765
XREF	CWE:189

Plugin Information:

Publication date: 2012/01/19, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.13

48245 - PHP 5.3 < 5.3.3 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.3. Such versions may be affected by several security issues :

- An error exists when processing invalid XML-RPC requests that can lead to a NULL pointer dereference. (bug #51288) (CVE-2010-0397)

- An error exists in the function 'shm_put_var' that is related to resource destruction.

- An error exists in the function 'fnmatch' that can lead to stack exhaustion. (CVE-2010-1917)

- A memory corruption error exists related to call-time pass by reference and callbacks.

- The dechunking filter is vulnerable to buffer overflow.

- An error exists in the sqlite extension that could allow arbitrary memory access.

- An error exists in the 'phar' extension related to string format validation.

- The functions 'mysqlnd_list_fields' and 'mysqlnd_change_user' are vulnerable to buffer overflow.

- The Mysqlnd extension is vulnerable to buffer overflow attack when handling error packets.

- The following functions are not properly protected against function interruptions :

addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query,

strpbrk, strtr, str_pad, str_word_count, wordwrap, strtok, setcookie, strip_tags, trim, ltrim, rtrim, substr_replace, parse_str, pack, unpack, uasort, preg_match, strrchr (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)

- The following opcodes are not properly protected against function interruptions :

ZEND_CONCAT, ZEND_ASSIGN_CONCAT, ZEND_FETCH_RW, XOR (CVE-2010-2191)

- The default session serializer contains an error that can be exploited when assigning session variables having user defined names. Arbitrary serialized values can be injected into sessions by including the PS_UNDEF_MARKER, '!', character in variable names.

- A use-after-free error exists in the function 'spl_object_storage_attach'. (CVE-2010-2225)

- An information disclosure vulnerability exists in the function 'var_export' when handling certain error conditions. (CVE-2010-2531)

See Also

http://www.php.net/releases/5_3_3.php
http://www.php.net/ChangeLog-5.php#5.3.3

Solution

Upgrade to PHP version 5.3.3 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	38708

BID	40461
BID	40948
BID	41991
CVE	CVE-2007-1581
CVE	CVE-2010-0397
CVE	CVE-2010-1860
CVE	CVE-2010-1862
CVE	CVE-2010-1864
CVE	CVE-2010-1917
CVE	CVE-2010-2097
CVE	CVE-2010-2100
CVE	CVE-2010-2101
CVE	CVE-2010-2190
CVE	CVE-2010-2191
CVE	CVE-2010-2225
CVE	CVE-2010-2484
CVE	CVE-2010-2531
CVE	CVE-2010-3062
CVE	CVE-2010-3063
CVE	CVE-2010-3064
CVE	CVE-2010-3065
XREF	OSVDB:33942
XREF	OSVDB:63078
XREF	OSVDB:64322
XREF	OSVDB:64544
XREF	OSVDB:64546
XREF	OSVDB:64607
XREF	OSVDB:65755
XREF	OSVDB:66087
XREF	OSVDB:66093
XREF	OSVDB:66094
XREF	OSVDB:66095
XREF	OSVDB:66096
XREF	OSVDB:66097
XREF	OSVDB:66098
XREF	OSVDB:66099
XREF	OSVDB:66100
XREF	OSVDB:66101
XREF	OSVDB:66102
XREF	OSVDB:66103
XREF	OSVDB:66104

XREF	OSVDB:66105
XREF	OSVDB:66106
XREF	OSVDB:66798
XREF	OSVDB:66804
XREF	OSVDB:66805
XREF	OSVDB:67418
XREF	OSVDB:67419
XREF	OSVDB:67420
XREF	OSVDB:67421
XREF	Secunia:39675
XREF	Secunia:40268

Plugin Information:

Publication date: 2010/08/04, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.3

51140 - PHP 5.3 < 5.3.4 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.4. Such versions may be affected by several security issues :

- A crash in the zip extract method.

- A stack-based buffer overflow in impagepstext() of the GD extension.

- An unspecified vulnerability related to symbolic resolution when using a DFS share.

- A security bypass vulnerability related to using pathnames containing NULL bytes.
(CVE-2006-7243)

- Multiple format string vulnerabilities.
(CVE-2010-2094, CVE-2010-2950)

- An unspecified security bypass vulnerability in open_basedir(). (CVE-2010-3436)

- A NULL pointer dereference in ZipArchive::getArchiveComment. (CVE-2010-3709)

- Memory corruption in php_filter_validate_email().
(CVE-2010-3710)

- An input validation vulnerability in xml_utf8_decode(). (CVE-2010-3870)

- A possible double free in the IMAP extension.
(CVE-2010-4150)

- An information disclosure vulnerability in 'mb_strcut()'. (CVE-2010-4156)

- An integer overflow vulnerability in 'getSymbol()'.
(CVE-2010-4409)

- A use-after-free vulnerability in the Zend engine when a '__set()', '__get()', '__isset()' or '__unset()'
method is called can allow for a denial of service attack. (Bug #52879 / CVE-2010-4697)

- A stack-based buffer overflow exists in the 'imagepstext()' function in the GD extension. (Bug #53492 / CVE-2010-4698)

- The 'iconv_mime_decode_headers()' function in the iconv extension fails to properly handle encodings that are not recognized by the iconv and mbstring implementations. (Bug #52941 / CVE-2010-4699)

- The 'set_magic_quotes_runtime()' function when the MySQLi extension is used does not properly interact with the 'mysqli_fetch_assoc()' function. (Bug #52221 / CVE-2010-4700)

- A race condition exists in the PCNTL extension.
(CVE-2011-0753)

- The SplFileInfo::getType function in the Standard PHP Library extension does not properly detect symbolic links. (CVE-2011-0754)

- An integer overflow exists in the mt_rand function.
(CVE-2011-0755)

See Also

http://www.php.net/releases/5_3_4.php
http://www.php.net/ChangeLog-5.php#5.3.4

Solution

Upgrade to PHP 5.3.4 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	40173
BID	43926
BID	44605
BID	44718
BID	44723
BID	44951
BID	44980
BID	45119
BID	45335
BID	45338
BID	45339
BID	45952
BID	45954
BID	46056
BID	46168
CVE	CVE-2006-7243
CVE	CVE-2010-2094
CVE	CVE-2010-2950
CVE	CVE-2010-3436

CVE	CVE-2010-3709
CVE	CVE-2010-3710
CVE	CVE-2010-3870
CVE	CVE-2010-4150
CVE	CVE-2010-4156
CVE	CVE-2010-4409
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2010-4699
CVE	CVE-2010-4700
CVE	CVE-2011-0753
CVE	CVE-2011-0754
CVE	CVE-2011-0755
XREF	OSVDB:66086
XREF	OSVDB:68597
XREF	OSVDB:69099
XREF	OSVDB:69109
XREF	OSVDB:69110
XREF	OSVDB:69230
XREF	OSVDB:69651
XREF	OSVDB:69660
XREF	OSVDB:70606
XREF	OSVDB:70607
XREF	OSVDB:70608
XREF	OSVDB:70609
XREF	OSVDB:70610
XREF	OSVDB:74193
XREF	OSVDB:74688
XREF	OSVDB:74689
XREF	CERT:479900

Plugin Information:

Publication date: 2010/12/13, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

Installed version : 5.3.0
Fixed version : 5.3.4

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
https://bugs.php.net/bug.php?id=61910
http://www.php.net/archive/2012.php#id2012-05-03-1
http://www.php.net/ChangeLog-5.php#5.3.12
http://www.php.net/ChangeLog-5.php#5.4.2

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS Base Score

8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	OSVDB:81633
XREF	OSVDB:82213
XREF	CERT:520827

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2012/05/04, Modification date: 2016/05/20

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.12 / 5.4.2

66842 - PHP 5.3.x < 5.3.26 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.26. It is, therefore, potentially affected by the following vulnerabilities:

- An error exists in the function 'php_quot_print_encode'

in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings (Bug #64879)

- An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c'
that could allow denial of service attacks. (Bug #64895)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?60cbc5f0
http://www.nessus.org/u?8456482e
http://www.php.net/ChangeLog-5.php#5.3.26

Solution

Apply the vendor patch or upgrade to PHP version 5.3.26 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	60411
BID	60731
CVE	CVE-2013-2110
CVE	CVE-2013-4635
XREF	OSVDB:93968
XREF	OSVDB:94063

Plugin Information:

Publication date: 2013/06/07, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.26

55925 - PHP 5.3 < 5.3.7 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x running on the remote host is prior to 5.3.7. It is, therefore, affected by the following vulnerabilities :

- A use-after-free vulnerability in substr_replace(). (CVE-2011-1148)

- A stack-based buffer overflow in socket_connect(). (CVE-2011-1938)

- A code execution vulnerability in ZipArchive::addGlob(). (CVE-2011-1657)

- crypt_blowfish was updated to 1.2. (CVE-2011-2483)

- Multiple NULL pointer dereferences. (CVE-2011-3182)

- An unspecified crash in error_log(). (CVE-2011-3267)

- A buffer overflow in crypt(). (CVE-2011-3268)

- A flaw exists in the php_win32_get_random_bytes() function when passing MCRYPT_DEV_URANDOM as source to mcrypt_create_iv(). A remote attacker can exploit this to cause a denial of service condition. (OSVDB 126477)

See Also

http://securityreason.com/achievement_securityalert/101
http://securityreason.com/exploitalert/10738
https://bugs.php.net/bug.php?id=54238
https://bugs.php.net/bug.php?id=54681
https://bugs.php.net/bug.php?id=54939
http://www.php.net/releases/5_3_7.php

Solution

Upgrade to PHP 5.3.7 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46843
BID	47950
BID	48259
BID	49241
BID	49249
BID	49252
CVE	CVE-2011-1148
CVE	CVE-2011-1657
CVE	CVE-2011-1938
CVE	CVE-2011-2202
CVE	CVE-2011-2483
CVE	CVE-2011-3182
CVE	CVE-2011-3267
CVE	CVE-2011-3268
XREF	OSVDB:72644
XREF	OSVDB:73113
XREF	OSVDB:73218

XREF	OSVDB:74738
XREF	OSVDB:74739
XREF	OSVDB:74742
XREF	OSVDB:74743
XREF	OSVDB:75200
XREF	OSVDB:126477
XREF	EDB-ID:17318
XREF	EDB-ID:17486

Plugin Information:

Publication date: 2011/08/22, Modification date: 2016/05/20

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.7

58966 - PHP < 5.3.11 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

- The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated.
(CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

http://www.nessus.org/u?e81d4026
https://bugs.php.net/bug.php?id=61043
https://bugs.php.net/bug.php?id=54374
https://bugs.php.net/bug.php?id=60227
http://marc.info/?l=oss-security&m=134626481806571&w=2
http://www.php.net/archive/2012.php#id2012-04-26-1
http://www.php.net/ChangeLog-5.php#5.3.11

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172
XREF	OSVDB:79017
XREF	OSVDB:81791
XREF	OSVDB:85086

Plugin Information:

Publication date: 2012/05/02, Modification date: 2013/10/23

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.11

77285 - PHP 5.3.x < 5.3.29 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)

- A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function 'cdf_read_short_sector'. (CVE-2014-0207)

- A flaw exists with the 'cdf_unpack_summary_info()' function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.
This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

- A flaw exists with the 'cdf_read_property_info()' function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

- A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

- An out-of-bounds read exists in printf. (Bug #67249)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.

See Also

http://php.net/archive/2014.php#id2014-08-14-1
http://www.php.net/ChangeLog-5.php#5.3.29

Solution

Upgrade to PHP version 5.3.29 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	64018
BID	67759
BID	67765
BID	67837
BID	68007
BID	68237

BID	68243
BID	69271
BID	73385
CVE	CVE-2013-6712
CVE	CVE-2014-0207
CVE	CVE-2014-0237
CVE	CVE-2014-0238
CVE	CVE-2014-3515
CVE	CVE-2014-3981
CVE	CVE-2014-4049
XREF	OSVDB:100440
XREF	OSVDB:107559
XREF	OSVDB:107560
XREF	OSVDB:107725
XREF	OSVDB:107994
XREF	OSVDB:108462
XREF	OSVDB:108463

Plugin Information:

Publication date: 2014/08/20, Modification date: 2015/03/30

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.29

52717 - PHP 5.3 < 5.3.6 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is older than 5.3.6.

- A NULL pointer can be dereferenced in the function '_zip_name_locate()' when processing empty archives and can lead to application crashes or code execution. Exploitation requires the 'ZIPARCHIVE::FL_UNCHANGED' setting to be in use. (CVE-2011-0421)

- A variable casting error exists in the Exif extention, which can allow denial of service attacks when handling crafted 'Image File Directory' (IFD) header values in the PHP function 'exif_read_data()'. Exploitation requires a 64bit system and a config setting 'memory_limit' above 4GB or unlimited. (CVE-2011-0708)

- An integer overflow vulnerability exists in the implementation of the PHP function 'shmop_read()' and can allow arbitrary code execution. (CVE-2011-1092)

- Errors exist in the file 'phar/phar_object.c' in which calls to 'zend_throw_exception_ex()' pass data as a string format parameter. This can lead to memory corruption when handling PHP archives (phar).
(CVE-2011-1153)

- A buffer overflow error exists in the C function 'xbuf_format_converter' when the PHP configuration value for 'precision' is set to a large value and can lead to application crashes. (CVE-2011-1464)

- An integer overflow error exists in the C function 'SdnToJulian()' in the Calendar extension and can lead to application crashes. (CVE-2011-1466)

- An unspecified error exists in the implementation of the PHP function 'numfmt_set_symbol()' and PHP method 'NumberFormatter::setSymbol()' in the Intl extension.
This error can lead to application crashes.
(CVE-2011-1467)

- Multiple memory leaks exist in the OpenSSL extension in the PHP functions 'openssl_encrypt' and 'openssl_decrypt'. (CVE-2011-1468)

- An unspecified error exists in the Streams component when accessing FTP URLs with an HTTP proxy.
(CVE-2011-1469)

- An integer signedness error and an unspecified error exist in the Zip extension and can lead to denial of service via certain ziparchive streams. (CVE-2011-1470, CVE-2011-1471)

- An unspecified error exists in the security enforcement regarding the parsing of the fastcgi protocol with the 'FastCGI Process Manager' (FPM) SAPI.

See Also

http://bugs.php.net/bug.php?id=54193

http://bugs.php.net/bug.php?id=54055
http://bugs.php.net/bug.php?id=53885
http://bugs.php.net/bug.php?id=53574
http://bugs.php.net/bug.php?id=53512
http://bugs.php.net/bug.php?id=54060
http://bugs.php.net/bug.php?id=54061
http://bugs.php.net/bug.php?id=54092
http://bugs.php.net/bug.php?id=53579
http://bugs.php.net/bug.php?id=49072
http://openwall.com/lists/oss-security/2011/02/14/1
http://www.php.net/releases/5_3_6.php
http://www.rooibo.com/2011/03/12/integer-overflow-en-php-2/

Solution

Upgrade to PHP 5.3.6 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46354
BID	46365
BID	46786
BID	46854
CVE	CVE-2011-0421
CVE	CVE-2011-0708
CVE	CVE-2011-1092
CVE	CVE-2011-1153
CVE	CVE-2011-1464
CVE	CVE-2011-1466
CVE	CVE-2011-1467

CVE	CVE-2011-1468
CVE	CVE-2011-1469
CVE	CVE-2011-1470
XREF	OSVDB:71597
XREF	OSVDB:71598
XREF	OSVDB:72531
XREF	OSVDB:72532
XREF	OSVDB:72533
XREF	OSVDB:73623
XREF	OSVDB:73624
XREF	OSVDB:73625
XREF	OSVDB:73626
XREF	OSVDB:73754
XREF	OSVDB:73755
XREF	EDB-ID:16261
XREF	Secunia:43328

Plugin Information:

Publication date: 2011/03/18, Modification date: 2016/05/20

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.6

59529 - PHP 5.3.x < 5.3.14 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.14, and is, therefore, potentially affected the following vulnerabilities :

- An integer overflow error exists in the function 'phar_parse_tarfile' in the file 'ext/phar/tar.c'. This error can lead to a heap-based buffer overflow when handling a maliciously crafted TAR file. Arbitrary code execution is possible due to this error. (CVE-2012-2386)

- A weakness exists in the 'crypt' function related to the DES implementation that can allow brute-force attacks. (CVE-2012-2143)

- Several design errors involving the incorrect parsing of PHP PDO prepared statements could lead to disclosure of sensitive information or denial of service. (CVE-2012-3450)

- A variable initialization error exists in the file 'ext/openssl/openssl.c' that can allow process memory contents to be disclosed when input data is of length zero. (CVE-2012-6113)

See Also

http://www.nessus.org/u?6adf7abc
https://bugs.php.net/bug.php?id=61755
http://www.php.net/ChangeLog-5.php#5.3.14
http://www.nessus.org/u?99140286
http://www.nessus.org/u?a42ad63a

Solution

Upgrade to PHP version 5.3.14 or later.

Risk Factor

High

CVSS Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

6.7 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	47545
BID	53729

BID	54777
BID	57462
CVE	CVE-2012-2143
CVE	CVE-2012-2386
CVE	CVE-2012-3450
CVE	CVE-2012-6113
XREF	OSVDB:72399
XREF	OSVDB:82510
XREF	OSVDB:82931
XREF	OSVDB:89424
XREF	EDB-ID:17201

Plugin Information:

Publication date: 2012/06/15, Modification date: 2013/12/04

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.14

57537 - PHP < 5.3.9 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)

- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)
- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that

can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)

- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)

- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)

- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption. (CVE-2012-0789)

See Also

https://www.tenable.com/security/research/tra-2012-01
http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5
http://www.php.net/archive/2012.php#id2012-01-11-1
http://archives.neohapsis.com/archives/bugtraq/2012-01/0092.html
https://bugs.php.net/bug.php?id=55475
https://bugs.php.net/bug.php?id=55776
https://bugs.php.net/bug.php?id=53502
http://www.php.net/ChangeLog-5.php#5.3.9

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	49754
BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379
CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	OSVDB:75713
XREF	OSVDB:77446
XREF	OSVDB:78115
XREF	OSVDB:78571
XREF	OSVDB:78676
XREF	OSVDB:79016
XREF	OSVDB:79332
XREF	TRA:TRA-2012-01

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2012/01/13, Modification date: 2015/10/07

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.9

59056 - PHP 5.3.x < 5.3.13 CGI Query String Code Execution [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.

The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
https://bugs.php.net/bug.php?id=61910
http://www.php.net/archive/2012.php#id2012-05-08-1
http://www.php.net/ChangeLog-5.php#5.3.13

Solution

Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS Base Score

8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

CVSS Temporal Score

7.2 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	OSVDB:81633
XREF	OSVDB:82213
XREF	CERT:520827

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2012/05/09, Modification date: 2013/10/30

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.13

67259 - PHP 5.3.x < 5.3.27 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.27. It is, therefore, potentially affected by the following vulnerabilities:

- A buffer overflow error exists in the function '_pdo_pgsql_error'. (Bug #64949)

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://bugs.php.net/64949
http://bugs.php.net/65236
http://www.php.net/ChangeLog-5.php#5.3.27

Solution

Apply the vendor patch or upgrade to PHP version 5.3.27 or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	61128
CVE	CVE-2013-4113
XREF	OSVDB:95152

Plugin Information:

Publication date: 2013/07/12, Modification date: 2016/05/20

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

Installed version : 5.3.0
Fixed version : 5.3.27

74363 - OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8za. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that could allow nonce disclosure via the 'FLUSH+RELOAD'
cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that could lead to execution of arbitrary code. Note this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists related to DTLS handshake handling that could lead to denial of service attacks. Note this issue only affects OpenSSL when used as a DTLS client. (CVE-2014-0221)

- An unspecified error exists that could allow an attacker to cause usage of weak keying material leading to simplified man-in-the-middle attacks.
(CVE-2014-0224)

- An unspecified error exists related to anonymous ECDH ciphersuites that could allow denial of service attacks. Note this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

See Also

http://www.openssl.org/news/vulnerabilities.html#2014-0076
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470
https://www.openssl.org/news/secadv/20140605.txt
http://ccsinjection.lepidum.co.jp/
https://www.imperialviolet.org/2014/06/05/earlyccs.html

Solution

Upgrade to OpenSSL 0.9.8za or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	66363
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	OSVDB:104810
XREF	OSVDB:107729
XREF	OSVDB:107730
XREF	OSVDB:107731
XREF	OSVDB:107732
XREF	CERT:978508

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/06/06, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8za

57459 - OpenSSL < 0.9.8s Multiple Vulnerabilities [-/+]

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL older than 0.9.8s. Such versions have the following vulnerabilities :

- An error exists related to ECDSA signatures and binary curves. The implementation of curves over binary fields could allow a remote, unauthenticated attacker to determine private key material via timing attacks.
(CVE-2011-1945)

- The Datagram Transport Layer Security (DTLS) implementation is vulnerable to plaintext recovery attacks when decrypting in CBC mode. (CVE-2011-4108)

- A double-free error exists during a policy check failure if the flag 'X509_V_FLAG_POLICY_CHECK' is set.
(CVE-2011-4109)

- An error exists related to SSLv3.0 records that can lead to disclosure of uninitialized memory because the library does not clear all bytes used as block cipher padding. (CVE-2011-4576)

- An error exists related to RFC 3779 processing that can allow denial of service attacks. Note that this functionality is not enabled by default and must be configured at compile time via the 'enable-rfc3779'
option. (CVE-2011-4577)

- An error exists related to handshake restarts for server gated cryptography (SGC) that can allow denial of service attacks. (CVE-2011-4619)

See Also

http://openssl.org/news/secadv_20120104.txt
http://www.openssl.org/news/changelog.html
http://www.nessus.org/u?c0f10f36
http://eprint.iacr.org/2011/232.pdf
http://cvs.openssl.org/chngview?cn=21301

Solution

Upgrade to OpenSSL 0.9.8s or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	47888
CVE	CVE-2011-1945
CVE	CVE-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
XREF	OSVDB:74632
XREF	OSVDB:78186
XREF	OSVDB:78187
XREF	OSVDB:78188
XREF	OSVDB:78189
XREF	OSVDB:78190
XREF	OSVDB:78191
XREF	CERT:536044

Plugin Information:

Publication date: 2012/01/09, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8s

77086 - OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zb. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A memory double-free error exists related to handling DTLS packets that allows denial of service attacks.
(CVE-2014-3505)

- An unspecified error exists related to handling DTLS handshake messages that allows denial of service attacks due to large amounts of memory being consumed.
(CVE-2014-3506)

- A memory leak error exists related to handling specially crafted DTLS packets that allows denial of service attacks. (CVE-2014-3507)

- An error exists related to 'OBJ_obj2txt' and the pretty printing 'X509_name_*' functions which leak stack data, resulting in an information disclosure. (CVE-2014-3508)

- A NULL pointer dereference error exists related to handling anonymous ECDH cipher suites and crafted handshake messages that allow denial of service attacks against clients. (CVE-2014-3510)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html

https://www.openssl.org/news/secadv/20140806.txt
https://www.openssl.org/news/vulnerabilities.html

Solution

Upgrade to OpenSSL 0.9.8zb or later.

Risk Factor

High

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.9 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	69075
BID	69076
BID	69078
BID	69081
BID	69082
CVE	CVE-2014-3505
CVE	CVE-2014-3506
CVE	CVE-2014-3507
CVE	CVE-2014-3508
CVE	CVE-2014-3510
XREF	OSVDB:109891
XREF	OSVDB:109892
XREF	OSVDB:109893
XREF	OSVDB:109894
XREF	OSVDB:109895

Plugin Information:

Publication date: 2014/08/08, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zb

17766 - OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow [-/+]

Synopsis

The remote server is affected by a buffer overflow vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8p / 1.0.0b.

If a TLS server is multithreaded and uses the SSL cache, a remote attacker could trigger a buffer overflow and crash the server or run arbitrary code.

See Also

http://openssl.org/news/secadv_20101116.txt

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0b or later.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3864
XREF	OSVDB:69265

Plugin Information:

Publication date: 2012/01/04, Modification date: 2014/08/15

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8p

58799 - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption [-/+]

Synopsis

The remote host may be affected by a memory corruption vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue.
Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8v was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

See Also

http://openssl.org/news/secadv_20120419.txt

http://seclists.org/fulldisclosure/2012/Apr/210
http://openssl.org/news/secadv_20120424.txt
http://cvs.openssl.org/chngview?cn=22479
http://www.openssl.org/news/changelog.html

Solution

Upgrade to OpenSSL 0.9.8w or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	53158
BID	53212
CVE	CVE-2012-2110
CVE	CVE-2012-2131
XREF	OSVDB:81223
XREF	OSVDB:82110
XREF	EDB-ID:18756

Plugin Information:

Publication date: 2012/04/24, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

Reported version : 0.9.8k
Fixed version : 0.9.8w

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- An flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers.
This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding.
(CVE-2013-5704)

- An flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.zerodayinitiative.com/advisories/ZDI-14-236/
https://archive.apache.org/dist/httpd/CHANGES_2.2.29
http://httpd.apache.org/security/vulnerabilities_22.html
http://martin.swende.se/blog/HTTPChunked.html

Solution

Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	66550
BID	68678
BID	68742
BID	68745
CVE	CVE-2013-5704
CVE	CVE-2014-0118
CVE	CVE-2014-0226
CVE	CVE-2014-0231
XREF	OSVDB:105190
XREF	OSVDB:109216
XREF	OSVDB:109231
XREF	OSVDB:109234
XREF	EDB-ID:34133

Plugin Information:

Publication date: 2014/09/04, Modification date: 2016/05/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12

Fixed version : 2.2.29

42052 - Apache 2.2.x < 2.2.14 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.14. It is, therefore, 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.

See Also

http://www.securityfocus.com/advisories/17947
http://www.securityfocus.com/advisories/17959
http://www.nessus.org/u?e470f137
https://issues.apache.org/bugzilla/show_bug.cgi?id=47645
http://www.nessus.org/u?c34c4eda

Solution

Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.5 (CVSS2#E:ND/RL:ND/RC:C)

References

BID	36254
BID	36260
BID	36596
CVE	CVE-2009-2699
CVE	CVE-2009-3094
CVE	CVE-2009-3095
XREF	OSVDB:57851
XREF	OSVDB:57882
XREF	OSVDB:58879
XREF	Secunia:36549
XREF	CWE:264

Plugin Information:

Publication date: 2009/10/07, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.14

33822 - XAMPP Example Pages Detection [-/+]

Synopsis

The remote web server allows access to its example pages.

Description

The remote web server makes available example scripts from XAMPP, an easy-to-install Apache distribution containing MySQL, PHP, and Perl. Allowing access to

these examples is not recommended since some are known to disclose sensitive information about the remote host and others may be affected by vulnerabilities such as cross-site scripting issues. Additionally, some pages have known cross-site scripting, SQL injection, and local file inclusion vulnerabilities.

Solution

Consult XAMPP's documentation for information about securing the example pages as well as other applications if necessary.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin Information:

Publication date: 2008/08/05, Modification date: 2015/09/24

Ports

tcp/80

Nessus was able to access XAMPP's examples using the following URL :

http://192.168.15.120/xampp/index.php

10678 - Apache mod_info /server-info Information Disclosure [-/+]

Synopsis

The remote web server discloses information about its configuration.

Description

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

http://httpd.apache.org/docs/mod/mod_info.html

Solution

If required, update Apache's configuration file(s) to either disable mod_info or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF	OSVDB:562

Plugin Information:

Publication date: 2001/05/28, Modification date: 2013/01/25

Ports

tcp/80

42862 - PHP 5.3 < 5.3.1 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.1. Such versions may be affected by several security issues :

- Sanity checks are missing in exif processing.

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'.

- It is possible to bypass the 'open_basedir' configuration setting using

'posix_mkfifo()'.

- The 'safe_mode_include_dir' configuration setting may be ignored. (Bug #50063)

- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list.

- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

- An unspecified vulnerability affects the LCG entropy.

See Also

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

Solution

Upgrade to PHP version 5.3.1 or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	36554
BID	36555
BID	37079

BID	37138
CVE	CVE-2009-3557
CVE	CVE-2009-3559
CVE	CVE-2009-4017
CVE	CVE-2009-4018
CVE	CVE-2010-1128
XREF	OSVDB:58188
XREF	OSVDB:60434
XREF	OSVDB:60435
XREF	OSVDB:60436
XREF	OSVDB:60437
XREF	OSVDB:60438
XREF	OSVDB:60451
XREF	OSVDB:63323
XREF	Secunia:37412
XREF	CWE:264

Plugin Information:

Publication date: 2009/11/20, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.1

51439 - PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.

Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit.

See Also

http://bugs.php.net/bug.php?id=53632
http://www.php.net/distributions/test_bug53632.txt
http://www.php.net/releases/5_2_17.php
http://www.php.net/releases/5_3_5.php

Solution

Upgrade to PHP 5.2.17/5.3.5 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	45668
CVE	CVE-2010-4645
XREF	OSVDB:70370

Plugin Information:

Publication date: 2011/01/07, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.2.17/5.3.5

66584 - PHP 5.3.x < 5.3.23 Information Disclosure [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by an information disclosure vulnerability.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.23. It is, therefore, potentially affected by an information disclosure vulnerability.

The fix for CVE-2013-1643 was incomplete and an error still exists in the files 'ext/soap/php_xml.c' and 'ext/libxml/libxml.c' related to handling external entities. This error could cause PHP to parse remote XML documents defined by an attacker and could allow access to arbitrary files.

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?7c770707
http://www.php.net/ChangeLog-5.php#5.3.23

Solution

Upgrade to PHP version 5.3.23 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	62373
CVE	CVE-2013-1824
XREF	OSVDB:90922

Plugin Information:

Publication date: 2013/05/24, Modification date: 2014/08/30

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.23

64992 - PHP 5.3.x < 5.3.22 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.22. It is, therefore, potentially affected by the following vulnerabilities :

- An error exists in the file 'ext/soap/soap.c'
related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'
related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

Note that this plugin does not attempt to exploit the vulnerabilities but, instead

relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?2dcf53bd
http://www.nessus.org/u?889595b1
http://www.php.net/ChangeLog-5.php#5.3.22

Solution

Upgrade to PHP version 5.3.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	58224
BID	58766
CVE	CVE-2013-1635
CVE	CVE-2013-1643
XREF	OSVDB:90921
XREF	OSVDB:90922

Plugin Information:

Publication date: 2013/03/04, Modification date: 2013/11/22

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.22

71426 - PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.28. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the PHP OpenSSL extension's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts. (CVE-2013-4073)

- A memory corruption flaw exists in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter. (CVE-2013-6420)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://seclists.org/fulldisclosure/2013/Dec/96
https://bugzilla.redhat.com/show_bug.cgi?id=1036830
http://www.nessus.org/u?b6ec9ef9
http://www.php.net/ChangeLog-5.php#5.3.28

Solution

Upgrade to PHP version 5.3.28 or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	60843
BID	64225
CVE	CVE-2013-4073
CVE	CVE-2013-6420
XREF	OSVDB:100979
XREF	OSVDB:94628
XREF	EDB-ID:30395

Plugin Information:

Publication date: 2013/12/14, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.28

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2
https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	65673
CVE	CVE-2012-1171
XREF	OSVDB:104201

Plugin Information:

Publication date: 2014/04/01, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.11 / 5.4.1

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.

- It may be possible to bypass the 'open_basedir'/ 'safe_mode' configuration restrictions due to an error in session extensions.

- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82
http://securityreason.com/securityalert/7008
http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.html
http://www.php.net/releases/5_3_2.php
http://www.php.net/ChangeLog-5.php#5.3.2
http://www.php.net/releases/5_2_13.php
http://www.php.net/ChangeLog-5.php#5.2.13

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

5.6 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	38182
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	OSVDB:62582
XREF	OSVDB:62583
XREF	OSVDB:63323
XREF	Secunia:38708

Plugin Information:

Publication date: 2010/02/26, Modification date: 2016/05/16

Ports

tcp/80

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.2 / 5.2.13

64532 - OpenSSL < 0.9.8y Multiple Vulnerabilities [-/+]

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL prior to 0.9.8y. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the handling of OCSP response verification that could allow denial of service attacks.
(CVE-2013-0166)

- An error exists related to the SSL/TLS/DTLS protocols, CBC mode encryption and response time. An attacker could obtain plaintext contents of encrypted traffic via timing attacks. (CVE-2013-0169)

See Also

https://www.openssl.org/news/secadv/20130204.txt

Solution

Upgrade to OpenSSL 0.9.8y or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	57778
BID	60268
CVE	CVE-2013-0166
CVE	CVE-2013-0169
XREF	OSVDB:89848
XREF	OSVDB:89865

Plugin Information:

Publication date: 2013/02/09, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8y

78552 - OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE) [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zc. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- An error exists related to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. A man-in-the-middle attacker can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. This is also known as the 'POODLE' issue. (CVE-2014-3566)

- An error exists related to session ticket handling that can allow denial of service attacks via memory leaks.
(CVE-2014-3567)

- An error exists related to the build configuration process and the 'no-ssl3' build option that allows servers and clients to process insecure SSL 3.0 handshake messages. (CVE-2014-3568)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html
https://www.openssl.org/news/secadv/20141015.txt
https://www.openssl.org/news/vulnerabilities.html
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Upgrade to OpenSSL 0.9.8zc or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
BID	70585
BID	70586
CVE	CVE-2014-3566
CVE	CVE-2014-3567
CVE	CVE-2014-3568
XREF	OSVDB:113251
XREF	OSVDB:113374
XREF	OSVDB:113377
XREF	CERT:577193

Plugin Information:

Publication date: 2014/10/17, Modification date: 2016/05/24

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zc

59076 - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service [-/+]

Synopsis

The remote host may be affected by a denial of service vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL 0.9.8 earlier than 0.9.8x. As such, the OpenSSL library itself is reportedly affected by a denial of service vulnerability.

An integer underflow error exists in the file 'ssl/d1_enc.c' in the function 'dtls1_enc'. When in CBC mode, DTLS record length values and explicit initialization vector length values related to DTLS packets are not handled properly, which can lead to memory corruption and application crashes.

See Also

http://openssl.org/news/secadv_20120510.txt
http://www.openssl.org/news/changelog.html
http://cvs.openssl.org/chngview?cn=22538
https://bugzilla.redhat.com/show_bug.cgi?id=820686

Solution

Upgrade to OpenSSL 0.9.8x or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53476

CVE	CVE-2012-2333
XREF	OSVDB:81810

Plugin Information:

Publication date: 2012/05/11, Modification date: 2014/08/15

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8x

82030 - OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zf. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A use-after-free condition exists in the d2i_ECPrivateKey() function due to improper processing of malformed EC private key files during import. A remote attacker can exploit this to dereference or free already freed memory, resulting in a denial of service or other unspecified impact. (CVE-2015-0209)

- An invalid read flaw exists in the ASN1_TYPE_cmp() function due to improperly performed boolean-type comparisons. A remote attacker can exploit this, via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature, to cause an invalid read operation, resulting in a denial of service. (CVE-2015-0286)

- A flaw exists in the ASN1_item_ex_d2i() function due to a failure to reinitialize 'CHOICE' and 'ADB' data structures when reusing a structure in ASN.1 parsing. This allows a remote attacker to cause an invalid write operation and memory corruption, resulting in a denial of service. (CVE-2015-0287)

- A NULL pointer dereference flaw exists in the X509_to_X509_REQ() function

due to improper processing of certificate keys. This allows a remote attacker, via a crafted X.509 certificate, to cause a denial of service. (CVE-2015-0288)

- A NULL pointer dereference flaw exists in the PKCS#7 parsing code due to incorrect handling of missing outer ContentInfo. This allows a remote attacker, using an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, to cause a denial of service. (CVE-2015-0289)

- A flaw exists in servers that both support SSLv2 and enable export cipher suites due to improper implementation of SSLv2. A remote attacker can exploit this, via a crafted CLIENT-MASTER-KEY message, to cause a denial of service. (CVE-2015-0293)

- A key disclosure vulnerability exists in the SSLv2 implementation in the get_client_master_key() function due to the acceptance of a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher. A man-in-the-middle attacker can exploit this to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle. (CVE-2016-0703)
- An information disclosure vulnerability exists in the SSLv2 implementation in the get_client_master_key() function due to incorrectly overwriting MASTER-KEY bytes during use of export cipher suites. A remote attacker can exploit this to create a Bleichenbacher oracle.
(CVE-2016-0704)

See Also

https://www.openssl.org/news/secadv/20150319.txt
https://www.openssl.org/news/secadv/20160301.txt

Solution

Upgrade to OpenSSL 0.9.8zf or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	73225
BID	73227
BID	73231
BID	73232
BID	73237
BID	73239
CVE	CVE-2015-0209
CVE	CVE-2015-0286
CVE	CVE-2015-0287
CVE	CVE-2015-0288
CVE	CVE-2015-0289
CVE	CVE-2015-0293
CVE	CVE-2016-0703
CVE	CVE-2016-0704
XREF	OSVDB:118817
XREF	OSVDB:119328
XREF	OSVDB:119755
XREF	OSVDB:119756
XREF	OSVDB:119757
XREF	OSVDB:119761
XREF	OSVDB:135152
XREF	OSVDB:135153

Plugin Information:

Publication date: 2015/03/24, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zf

17765 - OpenSSL < 0.9.8l Multiple Vulnerabilities [-/+]

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)

- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)

- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)

- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html
https://www.openssl.org/news/secadv/20090325.txt
http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html
http://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest
http://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest
http://cvs.openssl.org/chngview?cn=18187
http://cvs.openssl.org/chngview?cn=18188

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	OSVDB:52866
XREF	OSVDB:54612
XREF	OSVDB:54613
XREF	OSVDB:56752
XREF	EDB-ID:8720
XREF	CWE:310

Plugin Information:

Publication date: 2012/01/04, Modification date: 2016/05/20

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8l

84151 - OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zg. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A denial of service vulnerability exists when processing an ECParameters structure due to an infinite loop that occurs when a specified curve is over a

malformed binary polynomial field. A remote attacker can exploit this to perform a denial of service against any system that processes public keys, certificate requests, or certificates. This includes TLS clients and TLS servers with client authentication enabled. (CVE-2015-1788)

- A denial of service vulnerability exists due to improper validation of the content and length of the ASN1_TIME string by the X509_cmp_time() function. A remote attacker can exploit this, via a malformed certificate and CRLs of various sizes, to cause a segmentation fault, resulting in a denial of service condition. TLS clients that verify CRLs are affected.
TLS clients and servers with client authentication enabled may be affected if they use custom verification callbacks. (CVE-2015-1789)

- A NULL pointer dereference flaw exists in the PKCS#7 parsing code due to incorrect handling of missing inner 'EncryptedContent'. This allows a remote attacker, via specially crafted ASN.1-encoded PKCS#7 blobs with missing content, to cause a denial of service condition or other potential unspecified impacts. (CVE-2015-1790)

- A double-free error exists due to a race condition that occurs when a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket. (CVE-2015-1791)

- A denial of service vulnerability exists in the CMS code due to an infinite loop that occurs when verifying a signedData message. A remote attacker can exploit this to cause a denial of service condition. (CVE-2015-1792)

See Also

https://www.openssl.org/news/secadv/20150611.txt

Solution

Upgrade to OpenSSL 0.9.8gz or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	75154
BID	75156
BID	75157
BID	75158
BID	75161
CVE	CVE-2015-1788
CVE	CVE-2015-1789
CVE	CVE-2015-1790
CVE	CVE-2015-1791
CVE	CVE-2015-1792

Plugin Information:

Publication date: 2015/06/12, Modification date: 2015/09/01

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zg

80566 - OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK) [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zd. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A NULL pointer dereference flaw exists when the SSLv3 option isn't enabled and an SSLv3 ClientHello is received. This allows a remote attacker, using an unexpected handshake, to crash the daemon, resulting in a denial of service. (CVE-2014-3569)

- The BIGNUM squaring (BN_sqr) implementation does not properly calculate the square of a BIGNUM value. This allows remote attackers to defeat cryptographic protection mechanisms. (CVE-2014-3570)

- A NULL pointer dereference flaw exists with dtls1_get_record() when handling DTLS messages. A remote attacker, using a specially crafted DTLS message, can cause a denial of service. (CVE-2014-3571)

- A flaw exists with ECDH handshakes when using an ECDSA certificate without a ServerKeyExchange message. This allows a remote attacker to trigger a loss of forward secrecy from the ciphersuite. (CVE-2014-3572)

- A flaw exists when accepting non-DER variations of certificate signature algorithms and signature encodings due to a lack of enforcement of matches between signed and unsigned portions. A remote attacker, by including crafted data within a certificate's unsigned portion, can bypass fingerprint-based certificate-blacklist protection mechanisms. (CVE-2014-8275)

- A security feature bypass vulnerability, known as FREAK (Factoring attack on RSA-EXPORT Keys), exists due to the support of weak EXPORT_RSA cipher suites with keys less than or equal to 512 bits. A man-in-the-middle attacker may be able to downgrade the SSL/TLS connection to use EXPORT_RSA cipher suites which can be factored in a short amount of time, allowing the attacker to intercept and decrypt the traffic. (CVE-2015-0204)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html
https://www.openssl.org/news/secadv/20150108.txt
https://www.openssl.org/news/vulnerabilities.html
https://www.smacktls.com/#freak

Solution

Upgrade to OpenSSL 0.9.8zd or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	71934
BID	71935
BID	71936
BID	71937
BID	71939
BID	71942
CVE	CVE-2014-3569
CVE	CVE-2014-3570
CVE	CVE-2014-3571
CVE	CVE-2014-3572
CVE	CVE-2014-8275
CVE	CVE-2015-0204
XREF	OSVDB:116423
XREF	OSVDB:116792
XREF	OSVDB:116793
XREF	OSVDB:116794
XREF	OSVDB:116795
XREF	OSVDB:116796
XREF	CERT:243585

Plugin Information:

Publication date: 2015/01/16, Modification date: 2015/10/07

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zd

17767 - OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability [-/+]

Synopsis

The remote SSL layer is affected by a denial of service vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8p / 1.0.0e.

A remote attacker could crash client software when using ECDH. The impact of this vulnerability is not clear; arbitrary code could be run too.

Note that OpenSSL changelog only reports a fix for 0.9.8p. 1.0.0a is definitely vulnerable. Gentoo reports a fix for 1.0.0e but it covers other flaws.NVD reports 0.9.7 as vulnerable too but does not give any fixed version.

See Also

http://www.mail-archive.com/openssl-dev@openssl.org/msg28049.html

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0e or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	42306
CVE	CVE-2010-2939
XREF	OSVDB:66946
XREF	GLSA:201110-01

Plugin Information:

Publication date: 2012/01/04, Modification date: 2014/08/15

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8p

87219 - OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS [-/+]

Synopsis

The remote host is affected by a denial of service vulnerability.

Description

According to its banner, the remote host is running a version of OpenSSL 0.9.8 prior to 0.9.8zh. It is, therefore, affected by a flaw in the ASN1_TFLG_COMBINE implementation in file tasn_dec.c related to handling malformed X509_ATTRIBUTE structures. A remote attacker can exploit this to cause a memory leak by triggering a decoding failure in a PKCS#7 or CMS application, resulting in a denial of service.

See Also

https://www.openssl.org/news/secadv/20151203.txt

Solution

Upgrade to OpenSSL version 0.9.8zh or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2015-3195
XREF	OSVDB:131039

Plugin Information:

Publication date: 2015/12/07, Modification date: 2016/05/16

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zh

58564 - OpenSSL < 0.9.8u Multiple Vulnerabilities [-/+]

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses an OpenSSL version prior to 0.9.8u. As such, it is reportedly affected by the following vulnerabilities :

- An error exists in the function 'mime_hdr_cmp' that could allow a NULL pointer to be dereferenced when parsing certain MIME headers. (CVE-2006-7250)

- The fix for CVE-2011-4619 was not complete.

- An error exists in the Cryptographic Message Syntax (CMS) and PKCS #7 implementation such that data can be decrypted using Million Message Attack (MMA) adaptive chosen cipher text attack. (CVE-2012-0884)

- An error exists in the function 'mime_param_cmp' in the file 'crypto/asn1/asn_mime.c' that can allow a NULL pointer to be dereferenced when

handling certain S/MIME content. (CVE-2012-1165)

Note that SSL/TLS applications are not necessarily affected, but those using CMS, PKCS #7 and S/MIME decryption operations are.

See Also

http://marc.info/?l=openssl-dev&m=115685408414194&w=2
http://openssl.org/news/secadv_20120312.txt
http://www.openssl.org/news/changelog.html
http://www.openwall.com/lists/oss-security/2012/03/13/2
http://www.openwall.com/lists/oss-security/2012/02/28/14
http://www.nessus.org/u?4a3e3c8e
http://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8u or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	52181
BID	52428
BID	52764
CVE	CVE-2006-7250
CVE	CVE-2011-4619
CVE	CVE-2012-0884
CVE	CVE-2012-1165
XREF	OSVDB:78190

XREF	OSVDB:79650
XREF	OSVDB:80039
XREF	OSVDB:80040

Plugin Information:

Publication date: 2012/04/02, Modification date: 2016/05/12

Ports

tcp/80

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8u

10677 - Apache mod_status /server-status Information Disclosure [-/+]

Synopsis

The remote web server discloses information about its status.

Description

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

If required, update Apache's configuration file(s) to either disable mod_status or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF	OSVDB:561

Plugin Information:

Publication date: 2001/05/28, Modification date: 2014/05/05

Ports

tcp/80

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding. (CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.27
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected

modules are not in use.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	66303
CVE	CVE-2013-6438
CVE	CVE-2014-0098
XREF	OSVDB:104579
XREF	OSVDB:104580

Plugin Information:

Publication date: 2014/04/08, Modification date: 2015/10/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.27

53896 - Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS [-/+]

Synopsis

The remote web server may be affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr_fnmatch() function of the bundled APR library.

If mod_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.

Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.18
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Solution

Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	47820
CVE	CVE-2011-0419
XREF	OSVDB:73388
XREF	Secunia:44574

Plugin Information:

Publication date: 2011/05/13, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.18

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests.
(CVE-2013-1896)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.25
http://httpd.apache.org/security/vulnerabilities_22.html
http://www.nessus.org/u?f050c342

Solution

Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:UR)

References

BID	59826
BID	61129
CVE	CVE-2013-1862
CVE	CVE-2013-1896
XREF	OSVDB:93366
XREF	OSVDB:95498

Plugin Information:

Publication date: 2013/07/16, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.25

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars'
file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution.
(CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks.
(CVE-2012-2687)

Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.23 or later.

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53046
BID	55131
CVE	CVE-2012-0883
CVE	CVE-2012-2687
XREF	OSVDB:81359

XREF	OSVDB:84818
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Publication date: 2012/09/14, Modification date: 2015/10/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.23

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.
This could allow a remote attacker to indirectly send requests to intranet servers.
(CVE-2011-3368, CVE-2011-4317)

- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.
(CVE-2012-0021)

- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.
(CVE-2012-0031)

- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers.
(CVE-2012-0053)

- An error in the mod_proxy_ajp module when used to connect to a backend server that takes an overly long time to respond could lead to a temporary denial of service. (CVE-2012-4557)

Note that Nessus did not actually test for these flaws, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.22
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
BID	56753
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
CVE	CVE-2012-4557
XREF	OSVDB:76079
XREF	OSVDB:76744
XREF	OSVDB:77310
XREF	OSVDB:78293
XREF	OSVDB:78555
XREF	OSVDB:78556
XREF	OSVDB:89275

Plugin Information:

Publication date: 2012/02/02, Modification date: 2015/10/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.22

48205 - Apache 2.2.x < 2.2.16 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :

- A denial of service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)
- An information disclosure vulnerability in mod_proxy_ajp, mod_reqtimeout, and mod_proxy_http relating to timeout conditions. Note that this issue only affects Apache on Windows, Netware, and OS/2. (CVE-2010-2068)

Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=49246
https://issues.apache.org/bugzilla/show_bug.cgi?id=49417
http://www.nessus.org/u?ce8ac446

Solution

Upgrade to Apache version 2.2.16 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	40827
BID	41963
CVE	CVE-2010-1452
CVE	CVE-2010-2068
XREF	OSVDB:65654
XREF	OSVDB:66745
XREF	Secunia:40206

Plugin Information:

Publication date: 2010/07/30, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.16

50070 - Apache 2.2.x < 2.2.17 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :

- Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)

- An error exists in the 'apr_brigade_split_line' function in the bundled APR-util library. Carefully timed bytes in requests result in gradual memory increases leading to a denial of service. (CVE-2010-1623) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.17
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.17 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	37203
BID	36097
BID	43673
CVE	CVE-2009-3560
CVE	CVE-2009-3720
CVE	CVE-2010-1623
XREF	OSVDB:59737
XREF	OSVDB:60797
XREF	OSVDB:68327
XREF	Secunia:41701
XREF	CWE:119

Plugin Information:

Publication date: 2010/10/20, Modification date: 2015/10/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.17

56216 - Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS [-/+]

Synopsis

The remote web server is affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.21
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.21 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	49616
CVE	CVE-2011-3348
XREF	OSVDB:75647

Plugin Information:

Publication date: 2011/09/16, Modification date: 2016/05/04

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.21

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.24

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	58165
CVE	CVE-2012-3499
CVE	CVE-2012-4558
XREF	OSVDB:90556
XREF	OSVDB:90557
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864

XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Publication date: 2013/02/27, Modification date: 2015/10/19

Ports

tcp/80

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.24

11213 - HTTP TRACE / TRACK Methods Allowed [-/+]

Synopsis

Debugging functions are enabled on the remote web server.

Description

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

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/05/04

Ports

tcp/80

To disable these methods, add the following lines for each virtual host in your configuration file :

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

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request :

```
------------------------------ snip ------------------------------
TRACE /Nessus1007925785.html HTTP/1.1
Connection: Close
Host: 192.168.15.120
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

and received the following response from the remote server :

```
------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2016 19:09:41 GMT
Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k
mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1007925785.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.15.120
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure [-/+]

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php
http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51706
CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442

Plugin Information:

Publication date: 2012/02/02, Modification date: 2016/05/19

Ports

tcp/80

Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: 192.168.15.120
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.
Size of a request header field exceeds server limit.
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/80

Port 80/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/80

A web server is running on this port.

10107 - HTTP Server Type and Version [-/+]

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

The remote web server type is :

Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k
mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

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 Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Wed, 01 Jun 2016 19:08:58 GMT
Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
X-Powered-By: PHP/5.3.0
Location: http://192.168.15.120/xampp/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

48243 - PHP Version [-/+]

Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2014/10/31

Ports

tcp/80

Nessus was able to identify the following PHP version information :

Version : 5.3.0
Source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

57323 - OpenSSL Version Detection [-/+]

Synopsis

The version of OpenSSL can be identified.

Description

The version of OpenSSL could be extracted from the web server's banner. Note that in many cases, security patches are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2014/09/22

Ports

tcp/80

Source : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k

11424 - WebDAV Detection [-/+]

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information:

Publication date: 2003/03/20, Modification date: 2011/03/14

Ports

tcp/80

123/udp

10884 - Network Time Protocol (NTP) Server Detection [-/+]

Synopsis

An NTP server with an insecure configuration is listening on the remote host.

Description

An NTP server with an insecure configuration is listening on port 123.
It provides information about its version, current date, current time, and it may also provide system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2015/06/12

Ports

udp/123

Version : unknown

135/tcp

21655 - MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host has multiple bugs in its RPC/DCOM implementation (828741).

An attacker may exploit one of these flaws to execute arbitrary code on the remote system.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms04-012

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	10121
BID	10123

BID	10127
BID	8811
CVE	CVE-2003-0813
CVE	CVE-2004-0116
CVE	CVE-2003-0807
CVE	CVE-2004-0124
XREF	OSVDB:2670
XREF	OSVDB:5245
XREF	OSVDB:5246
XREF	OSVDB:5247
XREF	MSFT:MS04-012

Plugin Information:

Publication date: 2007/03/16, Modification date: 2013/11/04

Ports

tcp/135

10736 - DCE Services Enumeration [-/+]

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Local RPC service
Named pipe : keysvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe

Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Local RPC service
Named pipe : OLE3

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/135

Port 135/tcp was found to be open

135/udp

11890 - MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

A security vulnerability exists in the Messenger Service that could allow arbitrary code execution on an affected system. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system or could cause the Messenger Service to fail.
Disabling the Messenger Service will prevent the possibility of attack.

This plugin actually tests for the presence of this flaw.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms03-043

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	8826
CVE	CVE-2003-0717
XREF	OSVDB:10936
XREF	MSFT:MS03-043

Exploitable with

CANVAS (true)

Plugin Information:

Publication date: 2003/10/16, Modification date: 2016/01/14

Ports

udp/135

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not

itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/02/26

Ports

udp/137

The following 8 NetBIOS names have been gathered :

PC-VITTIMA = Computer name
WORKGROUP = Workgroup / Domain name
PC-VITTIMA = Messenger Service
PC-VITTIMA = File Server Service
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser
GEORGIA = Messenger Username

The remote host has the following MAC address on its adapter :

08:00:27:b8:40:cd

139/tcp

11011 - Microsoft Windows SMB Service Detection [-/+]

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc

between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

An SMB server is running on this port.

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/139

Port 139/tcp was found to be open

180/tcp

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/180

Port 180/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/180

A web server is running on this port.

10107 - HTTP Server Type and Version [-/+]

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/180

The remote web server type is :

Seattle Lab HTTP Server/1.0

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

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 Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/180

Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Server: Seattle Lab HTTP Server/1.0
Connection: close
Date: Wed, 01 Jun 2016 19:08:58 GMT
WWW-Authenticate: Basic realm="Administration"

443/tcp

58987 - PHP Unsupported Version Detection [-/+]

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2012/05/04, Modification date: 2015/10/06

Ports

tcp/443

Source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
End of support date : 2014/08/14
Announcement : http://php.net/archive/2014.php#id2014-08-14-1
Supported versions : 5.6.x / 5.5.x

60085 - PHP 5.3.x < 5.3.15 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.15, and is, therefore, potentially affected by the following vulnerabilities :

- An unspecified overflow vulnerability exists in the function '_php_stream_scandir' in the file 'main/streams/streams.c'. (CVE-2012-2688)

- An unspecified error exists that can allow the 'open_basedir' constraint to be bypassed.
(CVE-2012-3365)

See Also

http://www.php.net/ChangeLog-5.php#5.3.15

Solution

Upgrade to PHP version 5.3.15 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	54612
BID	54638
CVE	CVE-2012-2688
CVE	CVE-2012-3365
XREF	OSVDB:84100
XREF	OSVDB:84126

Plugin Information:

Publication date: 2012/07/20, Modification date: 2013/10/23

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.15

78555 - OpenSSL Unsupported [-/+]

Synopsis

The remote service is not a supported version.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html
http://www.nessus.org/u?4d55548d

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information:

Publication date: 2014/10/17, Modification date: 2016/01/06

Ports

tcp/443

Installed version : 0.9.8k
Supported versions : 1.0.2 / 1.0.1

45004 - Apache 2.2.x < 2.2.15 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :

- A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)

- The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)

- The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave call-backs in an undefined state. (CVE-2010-0425)

- A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)

- Added 'mod_reqtimeout' module to mitigate Slowloris attacks. (CVE-2007-6750)

See Also

http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
https://archive.apache.org/dist/httpd/CHANGES_2.2.15

Solution

Upgrade to Apache version 2.2.15 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	21865
BID	36935
BID	38491
BID	38494
BID	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XREF	OSVDB:59969
XREF	OSVDB:62674
XREF	OSVDB:62675
XREF	OSVDB:62676
XREF	Secunia:38776
XREF	CWE:200

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2010/10/20, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.15

57603 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow [-/+]

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

According to its self-reported banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr_palloc()' that could cause a heap overflow.

Note that the Apache HTTP server itself does not pass unsanitized, user-provided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache 2.2.13 or later.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	35949
CVE	CVE-2009-2412
XREF	OSVDB:56765
XREF	CWE:189

Plugin Information:

Publication date: 2012/01/19, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.13

48245 - PHP 5.3 < 5.3.3 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.3. Such versions may be affected by several security issues :

- An error exists when processing invalid XML-RPC requests that can lead to a NULL pointer dereference. (bug #51288) (CVE-2010-0397)

- An error exists in the function 'shm_put_var' that is related to resource destruction.

- An error exists in the function 'fnmatch' that can lead to stack exhaustion. (CVE-2010-1917)

- A memory corruption error exists related to call-time pass by reference and callbacks.

- The dechunking filter is vulnerable to buffer overflow.

- An error exists in the sqlite extension that could allow arbitrary memory access.

- An error exists in the 'phar' extension related to string format validation.

- The functions 'mysqlnd_list_fields' and 'mysqlnd_change_user' are vulnerable to buffer overflow.

- The Mysqlnd extension is vulnerable to buffer overflow attack when handling error packets.

- The following functions are not properly protected against function interruptions :

addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, strtr, str_pad, str_word_count, wordwrap, strtok, setcookie, strip_tags, trim, ltrim, rtrim, substr_replace, parse_str, pack, unpack, uasort, preg_match, strrchr (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)

- The following opcodes are not properly protected against function interruptions :

ZEND_CONCAT, ZEND_ASSIGN_CONCAT, ZEND_FETCH_RW, XOR (CVE-2010-2191)

- The default session serializer contains an error that can be exploited when assigning session variables having user defined names. Arbitrary serialized values can be injected into sessions by including the PS_UNDEF_MARKER, '!', character in variable names.

- A use-after-free error exists in the function 'spl_object_storage_attach'. (CVE-2010-2225)

- An information disclosure vulnerability exists in the function 'var_export' when handling certain error conditions. (CVE-2010-2531)

See Also

http://www.php.net/releases/5_3_3.php
http://www.php.net/ChangeLog-5.php#5.3.3

Solution

Upgrade to PHP version 5.3.3 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	38708
BID	40461
BID	40948
BID	41991
CVE	CVE-2007-1581
CVE	CVE-2010-0397

CVE	CVE-2010-1860
CVE	CVE-2010-1862
CVE	CVE-2010-1864
CVE	CVE-2010-1917
CVE	CVE-2010-2097
CVE	CVE-2010-2100
CVE	CVE-2010-2101
CVE	CVE-2010-2190
CVE	CVE-2010-2191
CVE	CVE-2010-2225
CVE	CVE-2010-2484
CVE	CVE-2010-2531
CVE	CVE-2010-3062
CVE	CVE-2010-3063
CVE	CVE-2010-3064
CVE	CVE-2010-3065
XREF	OSVDB:33942
XREF	OSVDB:63078
XREF	OSVDB:64322
XREF	OSVDB:64544
XREF	OSVDB:64546
XREF	OSVDB:64607
XREF	OSVDB:65755
XREF	OSVDB:66087
XREF	OSVDB:66093
XREF	OSVDB:66094
XREF	OSVDB:66095
XREF	OSVDB:66096
XREF	OSVDB:66097
XREF	OSVDB:66098
XREF	OSVDB:66099
XREF	OSVDB:66100
XREF	OSVDB:66101
XREF	OSVDB:66102
XREF	OSVDB:66103
XREF	OSVDB:66104
XREF	OSVDB:66105
XREF	OSVDB:66106
XREF	OSVDB:66798
XREF	OSVDB:66804
XREF	OSVDB:66805

XREF	OSVDB:67418
XREF	OSVDB:67419
XREF	OSVDB:67420
XREF	OSVDB:67421
XREF	Secunia:39675
XREF	Secunia:40268

Plugin Information:

Publication date: 2010/08/04, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.3

51140 - PHP 5.3 < 5.3.4 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.4. Such versions may be affected by several security issues :

- A crash in the zip extract method.

- A stack-based buffer overflow in impagepstext() of the GD extension.

- An unspecified vulnerability related to symbolic resolution when using a DFS share.

- A security bypass vulnerability related to using pathnames containing NULL bytes.
(CVE-2006-7243)

- Multiple format string vulnerabilities.
(CVE-2010-2094, CVE-2010-2950)

- An unspecified security bypass vulnerability in open_basedir(). (CVE-2010-3436)

- A NULL pointer dereference in ZipArchive::getArchiveComment. (CVE-2010-3709)

- Memory corruption in php_filter_validate_email().
(CVE-2010-3710)

- An input validation vulnerability in xml_utf8_decode(). (CVE-2010-3870)

- A possible double free in the IMAP extension.
(CVE-2010-4150)

- An information disclosure vulnerability in 'mb_strcut()'. (CVE-2010-4156)

- An integer overflow vulnerability in 'getSymbol()'.
(CVE-2010-4409)

- A use-after-free vulnerability in the Zend engine when a '__set()', '__get()', '__isset()' or '__unset()'
method is called can allow for a denial of service attack. (Bug #52879 / CVE-2010-4697)

- A stack-based buffer overflow exists in the 'imagepstext()' function in the GD extension. (Bug #53492 / CVE-2010-4698)

- The 'iconv_mime_decode_headers()' function in the iconv extension fails to properly handle encodings that are not recognized by the iconv and mbstring implementations. (Bug #52941 / CVE-2010-4699)

- The 'set_magic_quotes_runtime()' function when the MySQLi extension is used does not properly interact with the 'mysqli_fetch_assoc()' function. (Bug #52221 / CVE-2010-4700)

- A race condition exists in the PCNTL extension.
(CVE-2011-0753)

- The SplFileInfo::getType function in the Standard PHP Library extension does not properly detect symbolic links. (CVE-2011-0754)

- An integer overflow exists in the mt_rand function.
(CVE-2011-0755)

See Also

http://www.php.net/releases/5_3_4.php
http://www.php.net/ChangeLog-5.php#5.3.4

Solution

Upgrade to PHP 5.3.4 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	40173
BID	43926
BID	44605
BID	44718
BID	44723
BID	44951
BID	44980
BID	45119
BID	45335
BID	45338
BID	45339
BID	45952
BID	45954
BID	46056
BID	46168
CVE	CVE-2006-7243
CVE	CVE-2010-2094
CVE	CVE-2010-2950
CVE	CVE-2010-3436
CVE	CVE-2010-3709
CVE	CVE-2010-3710
CVE	CVE-2010-3870
CVE	CVE-2010-4150
CVE	CVE-2010-4156

CVE	CVE-2010-4409
CVE	CVE-2010-4697
CVE	CVE-2010-4698
CVE	CVE-2010-4699
CVE	CVE-2010-4700
CVE	CVE-2011-0753
CVE	CVE-2011-0754
CVE	CVE-2011-0755
XREF	OSVDB:66086
XREF	OSVDB:68597
XREF	OSVDB:69099
XREF	OSVDB:69109
XREF	OSVDB:69110
XREF	OSVDB:69230
XREF	OSVDB:69651
XREF	OSVDB:69660
XREF	OSVDB:70606
XREF	OSVDB:70607
XREF	OSVDB:70608
XREF	OSVDB:70609
XREF	OSVDB:70610
XREF	OSVDB:74193
XREF	OSVDB:74688
XREF	OSVDB:74689
XREF	CERT:479900

Plugin Information:

Publication date: 2010/12/13, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.4

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
https://bugs.php.net/bug.php?id=61910
http://www.php.net/archive/2012.php#id2012-05-03-1
http://www.php.net/ChangeLog-5.php#5.3.12
http://www.php.net/ChangeLog-5.php#5.4.2

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS Base Score

8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	OSVDB:81633
XREF	OSVDB:82213
XREF	CERT:520827

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2012/05/04, Modification date: 2016/05/20

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.12 / 5.4.2

66842 - PHP 5.3.x < 5.3.26 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.26. It is, therefore, potentially affected by the following vulnerabilities:

- An error exists in the function 'php_quot_print_encode'
in the file 'ext/standard/quot_print.c' that could allow a heap-based buffer overflow when attempting to parse certain strings (Bug #64879)

- An integer overflow error exists related to the value of 'JEWISH_SDN_MAX' in the file 'ext/calendar/jewish.c'

that could allow denial of service attacks. (Bug #64895)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?60cbc5f0
http://www.nessus.org/u?8456482e
http://www.php.net/ChangeLog-5.php#5.3.26

Solution

Apply the vendor patch or upgrade to PHP version 5.3.26 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	60411
BID	60731
CVE	CVE-2013-2110
CVE	CVE-2013-4635
XREF	OSVDB:93968
XREF	OSVDB:94063

Plugin Information:

Publication date: 2013/06/07, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.26

55925 - PHP 5.3 < 5.3.7 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x running on the remote host is prior to 5.3.7. It is, therefore, affected by the following vulnerabilities :

- A use-after-free vulnerability in substr_replace(). (CVE-2011-1148)

- A stack-based buffer overflow in socket_connect(). (CVE-2011-1938)

- A code execution vulnerability in ZipArchive::addGlob(). (CVE-2011-1657)

- crypt_blowfish was updated to 1.2. (CVE-2011-2483)

- Multiple NULL pointer dereferences. (CVE-2011-3182)

- An unspecified crash in error_log(). (CVE-2011-3267)

- A buffer overflow in crypt(). (CVE-2011-3268)

- A flaw exists in the php_win32_get_random_bytes() function when passing MCRYPT_DEV_URANDOM as source to mcrypt_create_iv(). A remote attacker can exploit this to cause a denial of service condition. (OSVDB 126477)

See Also

http://securityreason.com/achievement_securityalert/101
http://securityreason.com/exploitalert/10738
https://bugs.php.net/bug.php?id=54238

https://bugs.php.net/bug.php?id=54681
https://bugs.php.net/bug.php?id=54939
http://www.php.net/releases/5_3_7.php

Solution

Upgrade to PHP 5.3.7 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46843
BID	47950
BID	48259
BID	49241
BID	49249
BID	49252
CVE	CVE-2011-1148
CVE	CVE-2011-1657
CVE	CVE-2011-1938
CVE	CVE-2011-2202
CVE	CVE-2011-2483
CVE	CVE-2011-3182
CVE	CVE-2011-3267
CVE	CVE-2011-3268
XREF	OSVDB:72644
XREF	OSVDB:73113
XREF	OSVDB:73218
XREF	OSVDB:74738
XREF	OSVDB:74739
XREF	OSVDB:74742

XREF	OSVDB:74743
XREF	OSVDB:75200
XREF	OSVDB:126477
XREF	EDB-ID:17318
XREF	EDB-ID:17486

Plugin Information:

Publication date: 2011/08/22, Modification date: 2016/05/20

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.7

58966 - PHP < 5.3.11 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

- The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated.
(CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

http://www.nessus.org/u?e81d4026
https://bugs.php.net/bug.php?id=61043
https://bugs.php.net/bug.php?id=54374
https://bugs.php.net/bug.php?id=60227
http://marc.info/?l=oss-security&m=134626481806571&w=2
http://www.php.net/archive/2012.php#id2012-04-26-1
http://www.php.net/ChangeLog-5.php#5.3.11

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172
XREF	OSVDB:79017
XREF	OSVDB:81791
XREF	OSVDB:85086

Plugin Information:

Publication date: 2012/05/02, Modification date: 2013/10/23

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.11

77285 - PHP 5.3.x < 5.3.29 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.29. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer overflow error exists in the file 'ext/date/lib/parse_iso_intervals.c' related to handling DateInterval objects that allows denial of service attacks. (CVE-2013-6712)

- A boundary checking error exists related to the Fileinfo extension, Composite Document Format (CDF) handling, and the function 'cdf_read_short_sector'. (CVE-2014-0207)

- A flaw exists with the 'cdf_unpack_summary_info()' function within 'src/cdf.c' where multiple file_printf calls occur when handling specially crafted CDF files.
This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0237)

- A flaw exists with the 'cdf_read_property_info()' function within 'src/cdf.c' where an infinite loop occurs when handling specially crafted CDF files. This could allow a context dependent attacker to crash the web application using PHP. (CVE-2014-0238)

- A type-confusion error exists related to the Standard PHP Library (SPL) extension and the function 'unserialize'. (CVE-2014-3515)

- An error exists related to configuration scripts and temporary file handling that could allow insecure file usage. (CVE-2014-3981)

- A heap-based buffer overflow error exists related to the function 'dns_get_record' that could allow execution of arbitrary code. (CVE-2014-4049)

- An out-of-bounds read exists in printf. (Bug #67249)

Note that Nessus has not attempted to exploit these issues, but has instead relied only on the application's self-reported version number.

Additionally, note that version 5.3.29 marks the end of support for the PHP 5.3.x branch.

See Also

http://php.net/archive/2014.php#id2014-08-14-1
http://www.php.net/ChangeLog-5.php#5.3.29

Solution

Upgrade to PHP version 5.3.29 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	64018
BID	67759
BID	67765
BID	67837
BID	68007
BID	68237
BID	68243
BID	69271
BID	73385

CVE	CVE-2013-6712
CVE	CVE-2014-0207
CVE	CVE-2014-0237
CVE	CVE-2014-0238
CVE	CVE-2014-3515
CVE	CVE-2014-3981
CVE	CVE-2014-4049
XREF	OSVDB:100440
XREF	OSVDB:107559
XREF	OSVDB:107560
XREF	OSVDB:107725
XREF	OSVDB:107994
XREF	OSVDB:108462
XREF	OSVDB:108463

Plugin Information:

Publication date: 2014/08/20, Modification date: 2015/03/30

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.29

52717 - PHP 5.3 < 5.3.6 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is older than 5.3.6.

- A NULL pointer can be dereferenced in the function '_zip_name_locate()' when processing empty archives and can lead to application crashes or code execution. Exploitation requires the 'ZIPARCHIVE::FL_UNCHANGED'

setting to be in use. (CVE-2011-0421)

- A variable casting error exists in the Exif extention, which can allow denial of service attacks when handling crafted 'Image File Directory' (IFD) header values in the PHP function 'exif_read_data()'. Exploitation requires a 64bit system and a config setting 'memory_limit' above 4GB or unlimited. (CVE-2011-0708)

- An integer overflow vulnerability exists in the implementation of the PHP function 'shmop_read()' and can allow arbitrary code execution. (CVE-2011-1092)

- Errors exist in the file 'phar/phar_object.c' in which calls to 'zend_throw_exception_ex()' pass data as a string format parameter. This can lead to memory corruption when handling PHP archives (phar).
(CVE-2011-1153)

- A buffer overflow error exists in the C function 'xbuf_format_converter' when the PHP configuration value for 'precision' is set to a large value and can lead to application crashes. (CVE-2011-1464)

- An integer overflow error exists in the C function 'SdnToJulian()' in the Calendar extension and can lead to application crashes. (CVE-2011-1466)

- An unspecified error exists in the implementation of the PHP function 'numfmt_set_symbol()' and PHP method 'NumberFormatter::setSymbol()' in the Intl extension.
This error can lead to application crashes.
(CVE-2011-1467)

- Multiple memory leaks exist in the OpenSSL extension in the PHP functions 'openssl_encrypt' and 'openssl_decrypt'. (CVE-2011-1468)

- An unspecified error exists in the Streams component when accessing FTP URLs with an HTTP proxy.
(CVE-2011-1469)

- An integer signedness error and an unspecified error exist in the Zip extension and can lead to denial of service via certain ziparchive streams. (CVE-2011-1470, CVE-2011-1471)

- An unspecified error exists in the security enforcement regarding the parsing of the fastcgi protocol with the 'FastCGI Process Manager' (FPM) SAPI.

See Also

http://bugs.php.net/bug.php?id=54193
http://bugs.php.net/bug.php?id=54055
http://bugs.php.net/bug.php?id=53885
http://bugs.php.net/bug.php?id=53574
http://bugs.php.net/bug.php?id=53512

http://bugs.php.net/bug.php?id=54060
http://bugs.php.net/bug.php?id=54061
http://bugs.php.net/bug.php?id=54092
http://bugs.php.net/bug.php?id=53579
http://bugs.php.net/bug.php?id=49072
http://openwall.com/lists/oss-security/2011/02/14/1
http://www.php.net/releases/5_3_6.php
http://www.rooibo.com/2011/03/12/integer-overflow-en-php-2/

Solution

Upgrade to PHP 5.3.6 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46354
BID	46365
BID	46786
BID	46854
CVE	CVE-2011-0421
CVE	CVE-2011-0708
CVE	CVE-2011-1092
CVE	CVE-2011-1153
CVE	CVE-2011-1464
CVE	CVE-2011-1466
CVE	CVE-2011-1467
CVE	CVE-2011-1468
CVE	CVE-2011-1469
CVE	CVE-2011-1470
XREF	OSVDB:71597

XREF	OSVDB:71598
XREF	OSVDB:72531
XREF	OSVDB:72532
XREF	OSVDB:72533
XREF	OSVDB:73623
XREF	OSVDB:73624
XREF	OSVDB:73625
XREF	OSVDB:73626
XREF	OSVDB:73754
XREF	OSVDB:73755
XREF	EDB-ID:16261
XREF	Secunia:43328

Plugin Information:

Publication date: 2011/03/18, Modification date: 2016/05/20

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.6

59529 - PHP 5.3.x < 5.3.14 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.14, and is, therefore, potentially affected the following vulnerabilities :

- An integer overflow error exists in the function 'phar_parse_tarfile' in the file 'ext/phar/tar.c'. This error can lead to a heap-based buffer overflow when handling a maliciously crafted TAR file. Arbitrary code execution is possible due to this error. (CVE-2012-2386)

- A weakness exists in the 'crypt' function related to the DES implementation that can allow brute-force attacks. (CVE-2012-2143)

- Several design errors involving the incorrect parsing of PHP PDO prepared statements could lead to disclosure of sensitive information or denial of service. (CVE-2012-3450)

- A variable initialization error exists in the file 'ext/openssl/openssl.c' that can allow process memory contents to be disclosed when input data is of length zero. (CVE-2012-6113)

See Also

http://www.nessus.org/u?6adf7abc
https://bugs.php.net/bug.php?id=61755
http://www.php.net/ChangeLog-5.php#5.3.14
http://www.nessus.org/u?99140286
http://www.nessus.org/u?a42ad63a

Solution

Upgrade to PHP version 5.3.14 or later.

Risk Factor

High

CVSS Base Score

8.5 (CVSS2#AV:N/AC:M/Au:S/C:C/I:C/A:C)

CVSS Temporal Score

6.7 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	47545
BID	53729
BID	54777
BID	57462
CVE	CVE-2012-2143
CVE	CVE-2012-2386

CVE	CVE-2012-3450
CVE	CVE-2012-6113
XREF	OSVDB:72399
XREF	OSVDB:82510
XREF	OSVDB:82931
XREF	OSVDB:89424
XREF	EDB-ID:17201

Plugin Information:

Publication date: 2012/06/15, Modification date: 2013/12/04

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.14

57537 - PHP < 5.3.9 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)

- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)
- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an

attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)

- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)

- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)

- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption. (CVE-2012-0789)

See Also

https://www.tenable.com/security/research/tra-2012-01
http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5
http://www.php.net/archive/2012.php#id2012-01-11-1
http://archives.neohapsis.com/archives/bugtraq/2012-01/0092.html
https://bugs.php.net/bug.php?id=55475
https://bugs.php.net/bug.php?id=55776
https://bugs.php.net/bug.php?id=53502
http://www.php.net/ChangeLog-5.php#5.3.9

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	49754

BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379
CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	OSVDB:75713
XREF	OSVDB:77446
XREF	OSVDB:78115
XREF	OSVDB:78571
XREF	OSVDB:78676
XREF	OSVDB:79016
XREF	OSVDB:79332
XREF	TRA:TRA-2012-01

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2012/01/13, Modification date: 2015/10/07

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.9

59056 - PHP 5.3.x < 5.3.13 CGI Query String Code Execution [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x earlier than 5.3.13 and, as such, is potentially affected by a remote code execution and information disclosure vulnerability.

The fix for CVE-2012-1823 does not completely correct the CGI query vulnerability. Disclosure of PHP source code and code execution via query parameters are still possible.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
https://bugs.php.net/bug.php?id=61910
http://www.php.net/archive/2012.php#id2012-05-08-1
http://www.php.net/ChangeLog-5.php#5.3.13

Solution

Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite' workaround is available as well.

Risk Factor

High

CVSS Base Score

8.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)

CVSS Temporal Score

7.2 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	OSVDB:81633
XREF	OSVDB:82213
XREF	CERT:520827

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2012/05/09, Modification date: 2013/10/30

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.13

67259 - PHP 5.3.x < 5.3.27 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.27. It is, therefore, potentially affected by the following vulnerabilities:

- A buffer overflow error exists in the function '_pdo_pgsql_error'. (Bug #64949)

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead

relies only on PHP's self-reported version number.

See Also

http://bugs.php.net/64949
http://bugs.php.net/65236
http://www.php.net/ChangeLog-5.php#5.3.27

Solution

Apply the vendor patch or upgrade to PHP version 5.3.27 or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	61128
CVE	CVE-2013-4113
XREF	OSVDB:95152

Plugin Information:

Publication date: 2013/07/12, Modification date: 2016/05/20

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.27

74363 - OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8za. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that could allow nonce disclosure via the 'FLUSH+RELOAD'
cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that could lead to execution of arbitrary code. Note this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists related to DTLS handshake handling that could lead to denial of service attacks. Note this issue only affects OpenSSL when used as a DTLS client. (CVE-2014-0221)

- An unspecified error exists that could allow an attacker to cause usage of weak keying material leading to simplified man-in-the-middle attacks.
(CVE-2014-0224)

- An unspecified error exists related to anonymous ECDH ciphersuites that could allow denial of service attacks. Note this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

See Also

http://www.openssl.org/news/vulnerabilities.html#2014-0076
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470
https://www.openssl.org/news/secadv/20140605.txt
http://ccsinjection.lepidum.co.jp/
https://www.imperialviolet.org/2014/06/05/earlyccs.html

Solution

Upgrade to OpenSSL 0.9.8za or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	66363
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	OSVDB:104810
XREF	OSVDB:107729
XREF	OSVDB:107730
XREF	OSVDB:107731
XREF	OSVDB:107732
XREF	CERT:978508

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/06/06, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8za

57459 - OpenSSL < 0.9.8s Multiple Vulnerabilities [-/+]

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL older than 0.9.8s. Such versions have the following vulnerabilities :

- An error exists related to ECDSA signatures and binary curves. The implementation of curves over binary fields could allow a remote, unauthenticated attacker to determine private key material via timing attacks.
(CVE-2011-1945)

- The Datagram Transport Layer Security (DTLS) implementation is vulnerable to plaintext recovery attacks when decrypting in CBC mode. (CVE-2011-4108)

- A double-free error exists during a policy check failure if the flag 'X509_V_FLAG_POLICY_CHECK' is set.
(CVE-2011-4109)

- An error exists related to SSLv3.0 records that can lead to disclosure of uninitialized memory because the library does not clear all bytes used as block cipher padding. (CVE-2011-4576)

- An error exists related to RFC 3779 processing that can allow denial of service attacks. Note that this functionality is not enabled by default and must be configured at compile time via the 'enable-rfc3779'
option. (CVE-2011-4577)

- An error exists related to handshake restarts for server gated cryptography (SGC) that can allow denial of service attacks. (CVE-2011-4619)

See Also

http://openssl.org/news/secadv_20120104.txt
http://www.openssl.org/news/changelog.html

http://www.nessus.org/u?c0f10f36
http://eprint.iacr.org/2011/232.pdf
http://cvs.openssl.org/chngview?cn=21301

Solution

Upgrade to OpenSSL 0.9.8s or later.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	47888
CVE	CVE-2011-1945
CVE	CVE-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
XREF	OSVDB:74632
XREF	OSVDB:78186
XREF	OSVDB:78187
XREF	OSVDB:78188
XREF	OSVDB:78189
XREF	OSVDB:78190
XREF	OSVDB:78191
XREF	CERT:536044

Plugin Information:

Publication date: 2012/01/09, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8s

77086 - OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zb. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A memory double-free error exists related to handling DTLS packets that allows denial of service attacks.
(CVE-2014-3505)

- An unspecified error exists related to handling DTLS handshake messages that allows denial of service attacks due to large amounts of memory being consumed. (CVE-2014-3506)

- A memory leak error exists related to handling specially crafted DTLS packets that allows denial of service attacks. (CVE-2014-3507)

- An error exists related to 'OBJ_obj2txt' and the pretty printing 'X509_name_*' functions which leak stack data, resulting in an information disclosure. (CVE-2014-3508)

- A NULL pointer dereference error exists related to handling anonymous ECDH cipher suites and crafted handshake messages that allow denial of service attacks against clients. (CVE-2014-3510)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html
https://www.openssl.org/news/secadv/20140806.txt
https://www.openssl.org/news/vulnerabilities.html

Solution

Upgrade to OpenSSL 0.9.8zb or later.

Risk Factor

High

CVSS Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.9 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	69075
BID	69076
BID	69078
BID	69081
BID	69082
CVE	CVE-2014-3505
CVE	CVE-2014-3506
CVE	CVE-2014-3507
CVE	CVE-2014-3508
CVE	CVE-2014-3510
XREF	OSVDB:109891
XREF	OSVDB:109892
XREF	OSVDB:109893
XREF	OSVDB:109894
XREF	OSVDB:109895

Plugin Information:

Publication date: 2014/08/08, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zb

17766 - OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow [-/+]

Synopsis

The remote server is affected by a buffer overflow vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8p / 1.0.0b.

If a TLS server is multithreaded and uses the SSL cache, a remote attacker could trigger a buffer overflow and crash the server or run arbitrary code.

See Also

http://openssl.org/news/secadv_20101116.txt

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0b or later.

Risk Factor

High

CVSS Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

References

CVE	CVE-2010-3864
XREF	OSVDB:69265

Plugin Information:

Publication date: 2012/01/04, Modification date: 2014/08/15

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8p

58799 - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption [-/+]

Synopsis

The remote host may be affected by a memory corruption vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue.
Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8v was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

See Also

http://openssl.org/news/secadv_20120419.txt
http://seclists.org/fulldisclosure/2012/Apr/210
http://openssl.org/news/secadv_20120424.txt

http://cvs.openssl.org/chngview?cn=22479
http://www.openssl.org/news/changelog.html

Solution

Upgrade to OpenSSL 0.9.8w or later.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	53158
BID	53212
CVE	CVE-2012-2110
CVE	CVE-2012-2131
XREF	OSVDB:81223
XREF	OSVDB:82110
XREF	EDB-ID:18756

Plugin Information:

Publication date: 2012/04/24, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8w

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- An flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers.
This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding.
(CVE-2013-5704)

- An flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.zerodayinitiative.com/advisories/ZDI-14-236/
https://archive.apache.org/dist/httpd/CHANGES_2.2.29
http://httpd.apache.org/security/vulnerabilities_22.html
http://martin.swende.se/blog/HTTPChunked.html

Solution

Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	66550
BID	68678
BID	68742
BID	68745
CVE	CVE-2013-5704
CVE	CVE-2014-0118
CVE	CVE-2014-0226
CVE	CVE-2014-0231
XREF	OSVDB:105190
XREF	OSVDB:109216
XREF	OSVDB:109231
XREF	OSVDB:109234
XREF	EDB-ID:34133

Plugin Information:

Publication date: 2014/09/04, Modification date: 2016/05/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.29

42052 - Apache 2.2.x < 2.2.14 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.14. It is, therefore, 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.

See Also

http://www.securityfocus.com/advisories/17947
http://www.securityfocus.com/advisories/17959
http://www.nessus.org/u?e470f137
https://issues.apache.org/bugzilla/show_bug.cgi?id=47645
http://www.nessus.org/u?c34c4eda

Solution

Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.5 (CVSS2#E:ND/RL:ND/RC:C)

References

BID	36254
BID	36260
BID	36596
CVE	CVE-2009-2699
CVE	CVE-2009-3094
CVE	CVE-2009-3095
XREF	OSVDB:57851
XREF	OSVDB:57882
XREF	OSVDB:58879
XREF	Secunia:36549
XREF	CWE:264

Plugin Information:

Publication date: 2009/10/07, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.14

33822 - XAMPP Example Pages Detection [-/+]

Synopsis

The remote web server allows access to its example pages.

Description

The remote web server makes available example scripts from XAMPP, an easy-to-install Apache distribution containing MySQL, PHP, and Perl. Allowing access to these examples is not recommended since some are known to disclose sensitive information about the remote host and others may be affected by vulnerabilities

such as cross-site scripting issues. Additionally, some pages have known cross-site scripting, SQL injection, and local file inclusion vulnerabilities.

Solution

Consult XAMPP's documentation for information about securing the example pages as well as other applications if necessary.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin Information:

Publication date: 2008/08/05, Modification date: 2015/09/24

Ports

tcp/443

Nessus was able to access XAMPP's examples using the following URL :

https://192.168.15.120/xampp/index.php

10678 - Apache mod_info /server-info Information Disclosure [-/+]

Synopsis

The remote web server discloses information about its configuration.

Description

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

http://httpd.apache.org/docs/mod/mod_info.html

Solution

If required, update Apache's configuration file(s) to either disable mod_info or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF	OSVDB:562

Plugin Information:

Publication date: 2001/05/28, Modification date: 2013/01/25

Ports

tcp/443

42862 - PHP 5.3 < 5.3.1 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP 5.3 installed on the remote host is older than 5.3.1. Such versions may be affected by several security issues :

- Sanity checks are missing in exif processing.

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'.

- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'.

- The 'safe_mode_include_dir' configuration setting may be ignored. (Bug #50063)

- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list.

- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

- An unspecified vulnerability affects the LCG entropy.

See Also

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

Solution

Upgrade to PHP version 5.3.1 or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	36554
BID	36555
BID	37079
BID	37138

CVE	CVE-2009-3557
CVE	CVE-2009-3559
CVE	CVE-2009-4017
CVE	CVE-2009-4018
CVE	CVE-2010-1128
XREF	OSVDB:58188
XREF	OSVDB:60434
XREF	OSVDB:60435
XREF	OSVDB:60436
XREF	OSVDB:60437
XREF	OSVDB:60438
XREF	OSVDB:60451
XREF	OSVDB:63323
XREF	Secunia:37412
XREF	CWE:264

Plugin Information:

Publication date: 2009/11/20, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.1

51439 - PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.

Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit.

See Also

http://bugs.php.net/bug.php?id=53632
http://www.php.net/distributions/test_bug53632.txt
http://www.php.net/releases/5_2_17.php
http://www.php.net/releases/5_3_5.php

Solution

Upgrade to PHP 5.2.17/5.3.5 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	45668
CVE	CVE-2010-4645
XREF	OSVDB:70370

Plugin Information:

Publication date: 2011/01/07, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.2.17/5.3.5

66584 - PHP 5.3.x < 5.3.23 Information Disclosure [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by an information disclosure vulnerability.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.23. It is, therefore, potentially affected by an information disclosure vulnerability.

The fix for CVE-2013-1643 was incomplete and an error still exists in the files 'ext/soap/php_xml.c' and 'ext/libxml/libxml.c' related to handling external entities. This error could cause PHP to parse remote XML documents defined by an attacker and could allow access to arbitrary files.

Note that this plugin does not attempt to exploit the vulnerability, but instead relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?7c770707
http://www.php.net/ChangeLog-5.php#5.3.23

Solution

Upgrade to PHP version 5.3.23 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	62373
CVE	CVE-2013-1824
XREF	OSVDB:90922

Plugin Information:

Publication date: 2013/05/24, Modification date: 2014/08/30

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.23

64992 - PHP 5.3.x < 5.3.22 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.3.x installed on the remote host is prior to 5.3.22. It is, therefore, potentially affected by the following vulnerabilities :

- An error exists in the file 'ext/soap/soap.c'
related to the 'soap.wsdl_cache_dir' configuration directive and writing cache files that could allow remote 'wsdl' files to be written to arbitrary locations. (CVE-2013-1635)

- An error exists in the file 'ext/soap/php_xml.c'
related to parsing SOAP 'wsdl' files and external entities that could cause PHP to parse remote XML documents defined by an attacker. This could allow access to arbitrary files. (CVE-2013-1643)

Note that this plugin does not attempt to exploit the vulnerabilities but, instead

relies only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?2dcf53bd
http://www.nessus.org/u?889595b1
http://www.php.net/ChangeLog-5.php#5.3.22

Solution

Upgrade to PHP version 5.3.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	58224
BID	58766
CVE	CVE-2013-1635
CVE	CVE-2013-1643
XREF	OSVDB:90921
XREF	OSVDB:90922

Plugin Information:

Publication date: 2013/03/04, Modification date: 2013/11/22

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.22

71426 - PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is 5.3.x prior to 5.3.28. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the PHP OpenSSL extension's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts. (CVE-2013-4073)

- A memory corruption flaw exists in the way the openssl_x509_parse() function of the PHP OpenSSL extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious, self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function. This could cause the application to crash or possibly allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter. (CVE-2013-6420)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead relies only on PHP's self-reported version number.

See Also

http://seclists.org/fulldisclosure/2013/Dec/96
https://bugzilla.redhat.com/show_bug.cgi?id=1036830
http://www.nessus.org/u?b6ec9ef9
http://www.php.net/ChangeLog-5.php#5.3.28

Solution

Upgrade to PHP version 5.3.28 or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	60843
BID	64225
CVE	CVE-2013-4073
CVE	CVE-2013-6420
XREF	OSVDB:100979
XREF	OSVDB:94628
XREF	EDB-ID:30395

Plugin Information:

Publication date: 2013/12/14, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.28

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass [-/+]

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2
https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	65673
CVE	CVE-2012-1171
XREF	OSVDB:104201

Plugin Information:

Publication date: 2014/04/01, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.11 / 5.4.1

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.

- It may be possible to bypass the 'open_basedir'/ 'safe_mode' configuration restrictions due to an error in session extensions.

- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82
http://securityreason.com/securityalert/7008
http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.html
http://www.php.net/releases/5_3_2.php
http://www.php.net/ChangeLog-5.php#5.3.2
http://www.php.net/releases/5_2_13.php
http://www.php.net/ChangeLog-5.php#5.2.13

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

5.6 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	38182
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	OSVDB:62582
XREF	OSVDB:62583
XREF	OSVDB:63323
XREF	Secunia:38708

Plugin Information:

Publication date: 2010/02/26, Modification date: 2016/05/16

Ports

tcp/443

Version source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Installed version : 5.3.0
Fixed version : 5.3.2 / 5.2.13

64532 - OpenSSL < 0.9.8y Multiple Vulnerabilities [-/+]

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL prior to 0.9.8y. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the handling of OCSP response verification that could allow denial of service attacks.
(CVE-2013-0166)

- An error exists related to the SSL/TLS/DTLS protocols, CBC mode encryption and response time. An attacker could obtain plaintext contents of encrypted traffic via timing attacks. (CVE-2013-0169)

See Also

https://www.openssl.org/news/secadv/20130204.txt

Solution

Upgrade to OpenSSL 0.9.8y or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	57778
BID	60268
CVE	CVE-2013-0166
CVE	CVE-2013-0169
XREF	OSVDB:89848
XREF	OSVDB:89865

Plugin Information:

Publication date: 2013/02/09, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8y

78552 - OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE) [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zc. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- An error exists related to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. A man-in-the-middle attacker can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. This is also known as the 'POODLE' issue. (CVE-2014-3566)

- An error exists related to session ticket handling that can allow denial of service attacks via memory leaks.
(CVE-2014-3567)

- An error exists related to the build configuration process and the 'no-ssl3' build option that allows servers and clients to process insecure SSL 3.0 handshake messages. (CVE-2014-3568)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html
https://www.openssl.org/news/secadv/20141015.txt
https://www.openssl.org/news/vulnerabilities.html
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Upgrade to OpenSSL 0.9.8zc or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
BID	70585
BID	70586
CVE	CVE-2014-3566
CVE	CVE-2014-3567
CVE	CVE-2014-3568
XREF	OSVDB:113251
XREF	OSVDB:113374
XREF	OSVDB:113377
XREF	CERT:577193

Plugin Information:

Publication date: 2014/10/17, Modification date: 2016/05/24

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zc

59076 - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service [-/+]

Synopsis

The remote host may be affected by a denial of service vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL 0.9.8 earlier than 0.9.8x. As such, the OpenSSL library itself is reportedly affected by a denial of service vulnerability.

An integer underflow error exists in the file 'ssl/d1_enc.c' in the function 'dtls1_enc'. When in CBC mode, DTLS record length values and explicit initialization vector length values related to DTLS packets are not handled properly, which can lead to memory corruption and application crashes.

See Also

http://openssl.org/news/secadv_20120510.txt
http://www.openssl.org/news/changelog.html
http://cvs.openssl.org/chngview?cn=22538
https://bugzilla.redhat.com/show_bug.cgi?id=820686

Solution

Upgrade to OpenSSL 0.9.8x or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53476

CVE	CVE-2012-2333
XREF	OSVDB:81810

Plugin Information:

Publication date: 2012/05/11, Modification date: 2014/08/15

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8x

82030 - OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zf. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A use-after-free condition exists in the d2i_ECPrivateKey() function due to improper processing of malformed EC private key files during import. A remote attacker can exploit this to dereference or free already freed memory, resulting in a denial of service or other unspecified impact. (CVE-2015-0209)

- An invalid read flaw exists in the ASN1_TYPE_cmp() function due to improperly performed boolean-type comparisons. A remote attacker can exploit this, via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature, to cause an invalid read operation, resulting in a denial of service. (CVE-2015-0286)

- A flaw exists in the ASN1_item_ex_d2i() function due to a failure to reinitialize 'CHOICE' and 'ADB' data structures when reusing a structure in ASN.1 parsing. This allows a remote attacker to cause an invalid write operation and memory corruption, resulting in a denial of service. (CVE-2015-0287)

- A NULL pointer dereference flaw exists in the X509_to_X509_REQ() function

due to improper processing of certificate keys. This allows a remote attacker, via a crafted X.509 certificate, to cause a denial of service. (CVE-2015-0288)

- A NULL pointer dereference flaw exists in the PKCS#7 parsing code due to incorrect handling of missing outer ContentInfo. This allows a remote attacker, using an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, to cause a denial of service. (CVE-2015-0289)

- A flaw exists in servers that both support SSLv2 and enable export cipher suites due to improper implementation of SSLv2. A remote attacker can exploit this, via a crafted CLIENT-MASTER-KEY message, to cause a denial of service. (CVE-2015-0293)

- A key disclosure vulnerability exists in the SSLv2 implementation in the get_client_master_key() function due to the acceptance of a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher. A man-in-the-middle attacker can exploit this to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle. (CVE-2016-0703)
- An information disclosure vulnerability exists in the SSLv2 implementation in the get_client_master_key() function due to incorrectly overwriting MASTER-KEY bytes during use of export cipher suites. A remote attacker can exploit this to create a Bleichenbacher oracle.
(CVE-2016-0704)

See Also

https://www.openssl.org/news/secadv/20150319.txt
https://www.openssl.org/news/secadv/20160301.txt

Solution

Upgrade to OpenSSL 0.9.8zf or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

BID	73225
BID	73227
BID	73231
BID	73232
BID	73237
BID	73239
CVE	CVE-2015-0209
CVE	CVE-2015-0286
CVE	CVE-2015-0287
CVE	CVE-2015-0288
CVE	CVE-2015-0289
CVE	CVE-2015-0293
CVE	CVE-2016-0703
CVE	CVE-2016-0704
XREF	OSVDB:118817
XREF	OSVDB:119328
XREF	OSVDB:119755
XREF	OSVDB:119756
XREF	OSVDB:119757
XREF	OSVDB:119761
XREF	OSVDB:135152
XREF	OSVDB:135153

Plugin Information:

Publication date: 2015/03/24, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zf

17765 - OpenSSL < 0.9.8l Multiple Vulnerabilities [-/+]

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)

- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)

- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)

- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html
https://www.openssl.org/news/secadv/20090325.txt
http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html
http://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest
http://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest
http://cvs.openssl.org/chngview?cn=18187
http://cvs.openssl.org/chngview?cn=18188

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

4.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	OSVDB:52866
XREF	OSVDB:54612
XREF	OSVDB:54613
XREF	OSVDB:56752
XREF	EDB-ID:8720
XREF	CWE:310

Plugin Information:

Publication date: 2012/01/04, Modification date: 2016/05/20

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8l

84151 - OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zg. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A denial of service vulnerability exists when processing an ECParameters structure due to an infinite loop that occurs when a specified curve is over a

malformed binary polynomial field. A remote attacker can exploit this to perform a denial of service against any system that processes public keys, certificate requests, or certificates. This includes TLS clients and TLS servers with client authentication enabled. (CVE-2015-1788)

- A denial of service vulnerability exists due to improper validation of the content and length of the ASN1_TIME string by the X509_cmp_time() function. A remote attacker can exploit this, via a malformed certificate and CRLs of various sizes, to cause a segmentation fault, resulting in a denial of service condition. TLS clients that verify CRLs are affected.
TLS clients and servers with client authentication enabled may be affected if they use custom verification callbacks. (CVE-2015-1789)

- A NULL pointer dereference flaw exists in the PKCS#7 parsing code due to incorrect handling of missing inner 'EncryptedContent'. This allows a remote attacker, via specially crafted ASN.1-encoded PKCS#7 blobs with missing content, to cause a denial of service condition or other potential unspecified impacts. (CVE-2015-1790)

- A double-free error exists due to a race condition that occurs when a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket. (CVE-2015-1791)

- A denial of service vulnerability exists in the CMS code due to an infinite loop that occurs when verifying a signedData message. A remote attacker can exploit this to cause a denial of service condition. (CVE-2015-1792)

See Also

https://www.openssl.org/news/secadv/20150611.txt

Solution

Upgrade to OpenSSL 0.9.8gz or later.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	75154
BID	75156
BID	75157
BID	75158
BID	75161
CVE	CVE-2015-1788
CVE	CVE-2015-1789
CVE	CVE-2015-1790
CVE	CVE-2015-1791
CVE	CVE-2015-1792

Plugin Information:

Publication date: 2015/06/12, Modification date: 2015/09/01

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zg

80566 - OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK) [-/+]

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL 0.9.8 prior to 0.9.8zd. The OpenSSL library is, therefore, affected by the following vulnerabilities :

- A NULL pointer dereference flaw exists when the SSLv3 option isn't enabled and an SSLv3 ClientHello is received. This allows a remote attacker, using an unexpected handshake, to crash the daemon, resulting in a denial of service. (CVE-2014-3569)

- The BIGNUM squaring (BN_sqr) implementation does not properly calculate the square of a BIGNUM value. This allows remote attackers to defeat cryptographic protection mechanisms. (CVE-2014-3570)

- A NULL pointer dereference flaw exists with dtls1_get_record() when handling DTLS messages. A remote attacker, using a specially crafted DTLS message, can cause a denial of service. (CVE-2014-3571)

- A flaw exists with ECDH handshakes when using an ECDSA certificate without a ServerKeyExchange message. This allows a remote attacker to trigger a loss of forward secrecy from the ciphersuite. (CVE-2014-3572)

- A flaw exists when accepting non-DER variations of certificate signature algorithms and signature encodings due to a lack of enforcement of matches between signed and unsigned portions. A remote attacker, by including crafted data within a certificate's unsigned portion, can bypass fingerprint-based certificate-blacklist protection mechanisms. (CVE-2014-8275)

- A security feature bypass vulnerability, known as FREAK (Factoring attack on RSA-EXPORT Keys), exists due to the support of weak EXPORT_RSA cipher suites with keys less than or equal to 512 bits. A man-in-the-middle attacker may be able to downgrade the SSL/TLS connection to use EXPORT_RSA cipher suites which can be factored in a short amount of time, allowing the attacker to intercept and decrypt the traffic. (CVE-2015-0204)

See Also

https://www.openssl.org/news/openssl-0.9.8-notes.html
https://www.openssl.org/news/secadv/20150108.txt
https://www.openssl.org/news/vulnerabilities.html
https://www.smacktls.com/#freak

Solution

Upgrade to OpenSSL 0.9.8zd or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	71934
BID	71935
BID	71936
BID	71937
BID	71939
BID	71942
CVE	CVE-2014-3569
CVE	CVE-2014-3570
CVE	CVE-2014-3571
CVE	CVE-2014-3572
CVE	CVE-2014-8275
CVE	CVE-2015-0204
XREF	OSVDB:116423
XREF	OSVDB:116792
XREF	OSVDB:116793
XREF	OSVDB:116794
XREF	OSVDB:116795
XREF	OSVDB:116796
XREF	CERT:243585

Plugin Information:

Publication date: 2015/01/16, Modification date: 2015/10/07

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zd

17767 - OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability [-/+]

Synopsis

The remote SSL layer is affected by a denial of service vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8p / 1.0.0e.

A remote attacker could crash client software when using ECDH. The impact of this vulnerability is not clear; arbitrary code could be run too.

Note that OpenSSL changelog only reports a fix for 0.9.8p. 1.0.0a is definitely vulnerable. Gentoo reports a fix for 1.0.0e but it covers other flaws.NVD reports 0.9.7 as vulnerable too but does not give any fixed version.

See Also

http://www.mail-archive.com/openssl-dev@openssl.org/msg28049.html

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0e or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:ND)

References

BID	42306
CVE	CVE-2010-2939
XREF	OSVDB:66946
XREF	GLSA:201110-01

Plugin Information:

Publication date: 2012/01/04, Modification date: 2014/08/15

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8p

87219 - OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS [-/+]

Synopsis

The remote host is affected by a denial of service vulnerability.

Description

According to its banner, the remote host is running a version of OpenSSL 0.9.8 prior to 0.9.8zh. It is, therefore, affected by a flaw in the ASN1_TFLG_COMBINE implementation in file tasn_dec.c related to handling malformed X509_ATTRIBUTE structures. A remote attacker can exploit this to cause a memory leak by triggering a decoding failure in a PKCS#7 or CMS application, resulting in a denial of service.

See Also

https://www.openssl.org/news/secadv/20151203.txt

Solution

Upgrade to OpenSSL version 0.9.8zh or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2015-3195
XREF	OSVDB:131039

Plugin Information:

Publication date: 2015/12/07, Modification date: 2016/05/16

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8zh

58564 - OpenSSL < 0.9.8u Multiple Vulnerabilities [-/+]

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses an OpenSSL version prior to 0.9.8u. As such, it is reportedly affected by the following vulnerabilities :

- An error exists in the function 'mime_hdr_cmp' that could allow a NULL pointer to be dereferenced when parsing certain MIME headers. (CVE-2006-7250)

- The fix for CVE-2011-4619 was not complete.

- An error exists in the Cryptographic Message Syntax (CMS) and PKCS #7 implementation such that data can be decrypted using Million Message Attack (MMA) adaptive chosen cipher text attack. (CVE-2012-0884)

- An error exists in the function 'mime_param_cmp' in the file 'crypto/asn1/asn_mime.c' that can allow a NULL pointer to be dereferenced when

handling certain S/MIME content. (CVE-2012-1165)

Note that SSL/TLS applications are not necessarily affected, but those using CMS, PKCS #7 and S/MIME decryption operations are.

See Also

http://marc.info/?l=openssl-dev&m=115685408414194&w=2
http://openssl.org/news/secadv_20120312.txt
http://www.openssl.org/news/changelog.html
http://www.openwall.com/lists/oss-security/2012/03/13/2
http://www.openwall.com/lists/oss-security/2012/02/28/14
http://www.nessus.org/u?4a3e3c8e
http://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8u or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	52181
BID	52428
BID	52764
CVE	CVE-2006-7250
CVE	CVE-2011-4619
CVE	CVE-2012-0884
CVE	CVE-2012-1165
XREF	OSVDB:78190

XREF	OSVDB:79650
XREF	OSVDB:80039
XREF	OSVDB:80040

Plugin Information:

Publication date: 2012/04/02, Modification date: 2016/05/12

Ports

tcp/443

Banner : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k
Fixed version : 0.9.8u

10677 - Apache mod_status /server-status Information Disclosure [-/+]

Synopsis

The remote web server discloses information about its status.

Description

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

If required, update Apache's configuration file(s) to either disable mod_status or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF	OSVDB:561

Plugin Information:

Publication date: 2001/05/28, Modification date: 2014/05/05

Ports

tcp/443

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding. (CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.27
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected

modules are not in use.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	66303
CVE	CVE-2013-6438
CVE	CVE-2014-0098
XREF	OSVDB:104579
XREF	OSVDB:104580

Plugin Information:

Publication date: 2014/04/08, Modification date: 2015/10/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.27

53896 - Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS [-/+]

Synopsis

The remote web server may be affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr_fnmatch() function of the bundled APR library.

If mod_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.

Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.18
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Solution

Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	47820
CVE	CVE-2011-0419
XREF	OSVDB:73388
XREF	Secunia:44574

Plugin Information:

Publication date: 2011/05/13, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.18

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests.
(CVE-2013-1896)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.25
http://httpd.apache.org/security/vulnerabilities_22.html
http://www.nessus.org/u?f050c342

Solution

Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:UR)

References

BID	59826
BID	61129
CVE	CVE-2013-1862
CVE	CVE-2013-1896
XREF	OSVDB:93366
XREF	OSVDB:95498

Plugin Information:

Publication date: 2013/07/16, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.25

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars'
file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution.
(CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks.
(CVE-2012-2687)

Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.23 or later.

Risk Factor

Medium

CVSS Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

6.0 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	53046
BID	55131
CVE	CVE-2012-0883
CVE	CVE-2012-2687
XREF	OSVDB:81359

XREF	OSVDB:84818
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Publication date: 2012/09/14, Modification date: 2015/10/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.23

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.
This could allow a remote attacker to indirectly send requests to intranet servers.
(CVE-2011-3368, CVE-2011-4317)

- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.
(CVE-2012-0021)

- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.
(CVE-2012-0031)

- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers.
(CVE-2012-0053)

- An error in the mod_proxy_ajp module when used to connect to a backend server that takes an overly long time to respond could lead to a temporary denial of service. (CVE-2012-4557)

Note that Nessus did not actually test for these flaws, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.22
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
BID	56753
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
CVE	CVE-2012-4557
XREF	OSVDB:76079
XREF	OSVDB:76744
XREF	OSVDB:77310
XREF	OSVDB:78293
XREF	OSVDB:78555
XREF	OSVDB:78556
XREF	OSVDB:89275

Plugin Information:

Publication date: 2012/02/02, Modification date: 2015/10/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.22

48205 - Apache 2.2.x < 2.2.16 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :

- A denial of service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)
- An information disclosure vulnerability in mod_proxy_ajp, mod_reqtimeout, and mod_proxy_http relating to timeout conditions. Note that this issue only affects Apache on Windows, Netware, and OS/2. (CVE-2010-2068)

Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=49246
https://issues.apache.org/bugzilla/show_bug.cgi?id=49417
http://www.nessus.org/u?ce8ac446

Solution

Upgrade to Apache version 2.2.16 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	40827
BID	41963
CVE	CVE-2010-1452
CVE	CVE-2010-2068
XREF	OSVDB:65654
XREF	OSVDB:66745
XREF	Secunia:40206

Plugin Information:

Publication date: 2010/07/30, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.16

50070 - Apache 2.2.x < 2.2.17 Multiple Vulnerabilities [-/+]

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :

- Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)

- An error exists in the 'apr_brigade_split_line' function in the bundled APR-util library. Carefully timed bytes in requests result in gradual memory increases leading to a denial of service. (CVE-2010-1623) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.17
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.17 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	37203
BID	36097
BID	43673
CVE	CVE-2009-3560
CVE	CVE-2009-3720
CVE	CVE-2010-1623
XREF	OSVDB:59737
XREF	OSVDB:60797
XREF	OSVDB:68327
XREF	Secunia:41701
XREF	CWE:119

Plugin Information:

Publication date: 2010/10/20, Modification date: 2015/10/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.17

56216 - Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS [-/+]

Synopsis

The remote web server is affected by a denial of service vulnerability.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.21
http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.21 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	49616
CVE	CVE-2011-3348
XREF	OSVDB:75647

Plugin Information:

Publication date: 2011/09/16, Modification date: 2016/05/04

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.21

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities [-/+]

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.24

http://httpd.apache.org/security/vulnerabilities_22.html

Solution

Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	58165
CVE	CVE-2012-3499
CVE	CVE-2012-4558
XREF	OSVDB:90556
XREF	OSVDB:90557
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864

XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Publication date: 2013/02/27, Modification date: 2015/10/19

Ports

tcp/443

Version source : Server: Apache/2.2.12
Installed version : 2.2.12
Fixed version : 2.2.24

11213 - HTTP TRACE / TRACK Methods Allowed [-/+]

Synopsis

Debugging functions are enabled on the remote web server.

Description

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

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/05/04

Ports

tcp/443

To disable these methods, add the following lines for each virtual host in your configuration file :

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

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

```
------------------------------ snip ------------------------------
TRACE /Nessus299575003.html HTTP/1.1
Connection: Close
Host: 192.168.15.120
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

and received the following response from the remote server :

```
------------------------------ snip ------------------------------
HTTP/1.0 200 OK
Date: Wed, 01 Jun 2016 19:09:41 GMT
Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k
mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Connection: close
Content-Type: message/http


TRACE /Nessus299575003.html HTTP/1.1
Connection: Close
Host: 192.168.15.120
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database have been ignored.

See Also

http://tools.ietf.org/html/rfc3279
http://www.phreedom.org/research/rogue-ca/
http://technet.microsoft.com/en-us/security/advisory/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

3.5 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108
XREF	OSVDB:45127
XREF	CERT:836068

XREF CWE:310

Plugin Information:

Publication date: 2009/01/05, Modification date: 2015/09/22

Ports

tcp/443

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

|-Subject : CN=localhost
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Apr 15 22:04:42 2009 GMT
|-Valid To : Apr 13 22:04:42 2019 GMT

51192 - SSL Certificate Cannot Be Trusted [-/+]

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2015/10/21

Ports

tcp/443

The following certificate was at the top of the certificate chain sent by the remote host, but is signed by an unknown certificate authority :

|-Subject : CN=localhost
|-Issuer : CN=localhost

57582 - SSL Self-Signed Certificate [-/+]

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of

SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2015/10/21

Ports

tcp/443

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : CN=localhost

62565 - Transport Layer Security (TLS) Protocol CRIME Vulnerability [-/+]

Synopsis

The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description

The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

See Also

http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?8ec18eb5
https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Solution

Disable compression and / or the SPDY service.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	55704
BID	55707
CVE	CVE-2012-4929
CVE	CVE-2012-4930
XREF	OSVDB:85926
XREF	OSVDB:85927

Plugin Information:

Publication date: 2012/10/16, Modification date: 2014/09/26

Ports

tcp/443

The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

- SSL / TLS compression is enabled.

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of 'strong cryptography'.

See Also

http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2005/10/12, Modification date: 2015/10/07

Ports

tcp/443

- SSLv2 is enabled and the server supports at least one cipher.

- SSLv3 is enabled and the server supports at least one cipher.

26928 - SSL Weak Cipher Suites Supported [-/+]

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.openssl.org/docs/apps/ciphers.html

Solution

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

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Publication date: 2007/10/08, Modification date: 2014/12/30

Ports

tcp/443

Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 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-CBC(40) Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

The fields above are :

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.
Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Publication date: 2013/04/05, Modification date: 2015/10/07

Ports

tcp/443

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

SSLv2
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

TLSv1
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

High Strength Ciphers (>= 112-bit key)

SSLv2
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

TLSv1
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}

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) [-/+]

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

https://www.smacktls.com/#freak
https://www.openssl.org/news/secadv/20150108.txt
http://www.nessus.org/u?b78da2c4

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	71936
CVE	CVE-2015-0204
XREF	OSVDB:116794
XREF	CERT:243585

Plugin Information:

Publication date: 2015/03/04, Modification date: 2016/05/12

Ports

tcp/443

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

TLSv1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 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}

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) [-/+]

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	74733
CVE	CVE-2015-4000
XREF	OSVDB:122331

Plugin Information:

Publication date: 2015/05/21, Modification date: 2016/05/12

Ports

tcp/443

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40)
Mac=SHA1 export

The fields above are :

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

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) [-/+]

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Publication date: 2014/10/15, Modification date: 2016/01/26

Ports

tcp/443

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled

back" to SSLv3.

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) [-/+]

Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

See Also

https://drownattack.com/
https://drownattack.com/drown-attack-paper.pdf

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Risk Factor

Medium

CVSS Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

3.8 (CVSS2#E:F/RL:ND/RC:ND)

References

CVE	CVE-2016-0800
XREF	OSVDB:135149
XREF	CERT:583776

Plugin Information:

Publication date: 2016/03/01, Modification date: 2016/05/08

Ports

tcp/443

The remote host is affected by SSL DROWN and supports the following vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

High Strength Ciphers (>= 112-bit key)

SSLv2
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

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

45411 - SSL Certificate with Wrong Hostname [-/+]

Synopsis

The SSL certificate for this service is for a different host.

Description

The commonName (CN) of the SSL certificate presented on this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information:

Publication date: 2010/04/03, Modification date: 2014/03/11

Ports

tcp/443

The identities known by Nessus are :

192.168.15.120
192.168.15.120

The Common Name in the certificate is :

localhost

57792 - Apache HTTP Server httpOnly Cookie Information Disclosure [-/+]

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an

information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php
http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51706
CVE	CVE-2012-0053
XREF	OSVDB:78556
XREF	EDB-ID:18442

Plugin Information:

Publication date: 2012/02/02, Modification date: 2016/05/19

Ports

tcp/443

Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: 192.168.15.120
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.
Size of a request header field exceeds server limit.
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

http://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

BID	74733
CVE	CVE-2015-4000
XREF	OSVDB:122331

Plugin Information:

Publication date: 2015/05/28, Modification date: 2015/12/02

Ports

tcp/443

Vulnerable connection combinations :

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/443

Port 443/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/443

A TLSv1 server answered on this port.

tcp/443

A web server is running on this port through TLSv1.

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/443

A TLSv1 server answered on this port.

tcp/443

A web server is running on this port through TLSv1.

10107 - HTTP Server Type and Version [-/+]

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/443

The remote web server type is :

Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k
mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

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 Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/443

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Wed, 01 Jun 2016 19:08:58 GMT
Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
X-Powered-By: PHP/5.3.0
Location: https://192.168.15.120/xampp/
Content-Length: 0
Connection: close
Content-Type: text/html

48243 - PHP Version [-/+]

Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2014/10/31

Ports

tcp/443

Nessus was able to identify the following PHP version information :

Version : 5.3.0
Source : Server: Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0

57323 - OpenSSL Version Detection [-/+]

Synopsis

The version of OpenSSL can be identified.

Description

The version of OpenSSL could be extracted from the web server's banner. Note that in many cases, security patches are backported and the displayed version number

does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2014/09/22

Ports

tcp/443

Source : Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Reported version : 0.9.8k

11424 - WebDAV Detection [-/+]

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information:

Publication date: 2003/03/20, Modification date: 2011/03/14

Ports

tcp/443

56984 - SSL / TLS Versions Supported [-/+]

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2016/01/11

Ports

tcp/443

This port supports SSLv2/SSLv3/TLSv1.0.

62563 - SSL Compression Methods Supported [-/+]

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml
http://tools.ietf.org/html/rfc3749
http://tools.ietf.org/html/rfc3943
http://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2015/05/06

Ports

tcp/443

Nessus was able to confirm that the following compression method is supported by the target :

DEFLATE (0x01)

45410 - SSL Certificate commonName Mismatch [-/+]

Synopsis

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName' (CN) does not match the host name on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Publication date: 2010/04/03, Modification date: 2012/09/30

Ports

tcp/443

The host name known by Nessus is :

pc-vittima

The Common Name in the certificate is :

localhost

21643 - SSL Cipher Suites Supported [-/+]

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/manmaster/apps/ciphers.html
http://www.nessus.org/u?7d537016

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2015/08/27

Ports

tcp/443

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
Low Strength Ciphers (<= 64-bit key)
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1

AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

SSL Version : SSLv3
Low Strength Ciphers (<= 64-bit key)
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

SSL Version : SSLv2
Low Strength Ciphers (<= 64-bit key)
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

High Strength Ciphers (>= 112-bit key)
DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=MD5
RC2-CBC-MD5 Kx=RSA Au=RSA Enc=RC2-CBC(128) Mac=MD5
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

http://www.openssl.org/docs/apps/ciphers.html
http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/443

Here is the list of SSL PFS ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)

TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

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

51891 - SSL Session Resume Supported [-/+]

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports

tcp/443

This port supports resuming SSLv3 sessions.

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

http://www.openssl.org/docs/apps/ciphers.html
http://www.nessus.org/u?cc4a822a
http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/443

Here is the list of SSL CBC ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

SSLv2

DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5
export

TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES-CBC(40)
Mac=SHA1 export
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES-CBC(56) Mac=SHA1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES-CBC(40) Mac=SHA1
export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5
export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

High Strength Ciphers (>= 112-bit key)

SSLv2
DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=MD5
RC2-CBC-MD5 Kx=RSA Au=RSA Enc=RC2-CBC(128) Mac=MD5

TLSv1
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES-CBC(168) Mac=SHA1
DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES-CBC(128) Mac=SHA1
DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES-CBC(256) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES-CBC(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES-CBC(256) Mac=SHA1

The fields above are :

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

84502 - HSTS Missing From HTTPS Server [-/+]

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information:

Publication date: 2015/07/02, Modification date: 2015/07/02

Ports

tcp/443

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.

10863 - SSL Certificate Information [-/+]

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 Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/443

Subject Name:

Common Name: localhost

Issuer Name:

Common Name: localhost

Serial Number: 00 B3 32 F0 DC 69 65 8D FA

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 15 22:04:42 2009 GMT
Not Valid After: Apr 13 22:04:42 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 CD FA AD 98 F5 8E 74 16 F0 0A AB C6 0A C8 D0 00 4B 66 F9
76 06 06 8D D8 4A 1E 02 0D 7A F5 DB 50 74 D2 ED 5D 91 24 77
DC 2C 9C 93 46 75 1F 20 D3 9F 07 24 0E 5B AC 20 A8 C7 0D E4
EE 45 80 0A DB 75 42 58 13 19 9B 6C 36 9E 14 33 B2 CC 8F 0C
EB C5 BA B6 AD EA 10 65 D7 39 66 F0 21 88 07 38 7A 0E C8 2A
65 CA F3 14 0A 5E 2C 42 90 CC 84 43 E5 66 BA 60 46 B4 DB B2
87 73 15 43 A9 D3 29 45 85
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 30 B6 DB 36 B9 D5 2D 0F 30 E9 64 79 32 4B 94 DD A8 8F 4D
77 9D AD 59 56 D8 20 75 8F 92 B1 8B 1A 61 50 71 30 48 70 10
8C B6 4F 3B A8 19 2B A9 EB 82 32 89 0F 00 02 1D AD EF 69 B0
A7 4B 1F 3A 3A 22 1A 7F 01 AE 65 30 00 D3 46 7C CF 66 CA 2C
FD E9 96 01 A5 A2 51 45 50 B0 FE 2D 78 56 4F 4F 93 E3 9C E5
4D D3 A2 DD 0E E1 1A D2 71 D2 24 7D 55 30 46 39 8D 54 2C AB
76 93 F8 8F 37 BE 0D 0D C1

Fingerprints :

SHA-256 Fingerprint: 10 17 42 26 ED 55 F7 8D BF F9 0A 0E 5F 53 5D 95 90 3E 24 1B
AA 33 A0 3C 29 43 43 82 7F DA 71 B4
SHA-1 Fingerprint: E4 8B DD 08 16 E9 6D BE 01 4C 4C 9D 51 63 2C 93 F7 76 A4 86
MD5 Fingerprint: CB 7E 4C 94 24 78 A7 00 63 75 B3 81 3D 00 22 A8

50845 - OpenSSL Detection [-/+]

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/443

445/tcp

35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) [-/+]

Synopsis

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

Description

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

See Also

http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	31179
BID	33121
BID	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
XREF	OSVDB:48153

XREF	OSVDB:52691
XREF	OSVDB:52692
XREF	MSFT:MS09-001
XREF	CWE:399

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2009/01/13, Modification date: 2016/04/27

Ports

tcp/445

19408 - MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the Plug-And-Play service.

Description

The remote version of Windows contains a flaw in the function 'PNP_QueryResConfList()' in the Plug and Play service that may allow an attacker to execute arbitrary code on the remote host with SYSTEM privileges.

A series of worms (Zotob) are known to exploit this vulnerability in the wild.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms05-039

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	14513
CVE	CVE-2005-1983
XREF	OSVDB:18605
XREF	MSFT:MS05-039

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2005/08/09, Modification date: 2014/03/31

Ports

tcp/445

22194 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to a buffer overrun in the 'Server'
service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms06-040

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	19409
CVE	CVE-2006-3439
XREF	OSVDB:27845
XREF	MSFT:MS06-040

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2006/08/08, Modification date: 2014/03/31

Ports

tcp/445

11835 - MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is running a version of Windows that has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges.

An attacker or a worm could use it to gain the control of this host.

Note that this is NOT the same bug as the one described in MS03-026, which fixes the flaw exploited by the 'MSBlast' (or LoveSan) worm.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms03-039

Solution

Microsoft has released patches for Windows NT, 2000, XP, and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	8458
BID	8460
CVE	CVE-2003-0715
CVE	CVE-2003-0528
CVE	CVE-2003-0605
XREF	OSVDB:11460

XREF	OSVDB:11797
XREF	OSVDB:2535
XREF	MSFT:MS03-039

Plugin Information:

Publication date: 2003/09/10, Modification date: 2014/07/11

Ports

tcp/445

19407 - MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the Spooler service.

Description

The remote host contains a version of the Print Spooler service that may allow an attacker to execute code on the remote host or crash the spooler service.

An attacker can execute code on the remote host with a NULL session against :

- Windows 2000

An attacker can crash the remote service with a NULL session against :

- Windows 2000
- Windows XP SP1

An attacker needs valid credentials to crash the service against :

- Windows 2003
- Windows XP SP2

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms05-043

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	14514
CVE	CVE-2005-1984
XREF	OSVDB:18607
XREF	MSFT:MS05-043

Exploitable with

CANVAS (true)Core Impact (true)

Plugin Information:

Publication date: 2005/08/09, Modification date: 2013/11/04

Ports

tcp/445

12054 - MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote Windows host has an ASN.1 library that could allow an attacker to execute arbitrary code on this host.

To exploit this flaw, an attacker would need to send a specially crafted ASN.1 encoded packet with improperly advertised lengths.

This particular check sent a malformed NTLM packet and determined that the remote host is not patched.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms04-007

Solution

Microsoft has released patches for Windows NT, 2000, XP, and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	9633
BID	9635
BID	9743
BID	13300
CVE	CVE-2003-0818
XREF	OSVDB:3902
XREF	MSFT:MS04-007

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2004/02/13, Modification date: 2016/05/04

Ports

tcp/445

47556 - MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check) [-/+]

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by several vulnerabilities in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

These vulnerabilities depend on access to a shared drive, but do not necessarily require credentials.

See Also

http://technet.microsoft.com/en-us/security/bulletin/MS10-012

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	38049
BID	38051
BID	38054
BID	38085
CVE	CVE-2010-0020
CVE	CVE-2010-0021
CVE	CVE-2010-0022
CVE	CVE-2010-0231
XREF	OSVDB:62253
XREF	OSVDB:62254
XREF	OSVDB:62255
XREF	OSVDB:62256
XREF	MSFT:MS10-012
XREF	CWE:310
XREF	CWE:264

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2010/09/13, Modification date: 2013/11/04

Ports

tcp/445

48405 - MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check) [-/+]

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by several vulnerabilities in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. These vulnerabilities depend on access to a shared drive, but do not necessarily require credentials.

See Also

http://technet.microsoft.com/en-us/security/bulletin/MS10-054

Solution

Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	42224
BID	42263
BID	42267
CVE	CVE-2010-2550
CVE	CVE-2010-2551
CVE	CVE-2010-2552
XREF	OSVDB:66974
XREF	OSVDB:66975
XREF	OSVDB:66976
XREF	EDB-ID:14607
XREF	MSFT:MS10-054

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2010/08/23, Modification date: 2015/01/13

Ports

tcp/445

53503 - MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check) [-/+]

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by a vulnerability in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. This vulnerability depends on access to a Windows file share, but does not necessarily require credentials.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-020

Solution

Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	47198
CVE	CVE-2011-0661
XREF	OSVDB:71781
XREF	IAVA:2011-A-0050
XREF	MSFT:MS11-020

Plugin Information:

Publication date: 2011/04/20, Modification date: 2013/11/04

Ports

tcp/445

12209 - MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the LSASS service.

Description

The remote version of Windows contains a flaw in the function ' DsRolerUpgradeDownlevelServer' of the Local Security Authority Server Service (LSASS) that allows an attacker to execute arbitrary code on the remote host with SYSTEM privileges.

A series of worms (Sasser) are known to exploit this vulnerability in the wild.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms04-011

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	10108
CVE	CVE-2003-0533
XREF	OSVDB:5248
XREF	MSFT:MS04-011

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2004/04/15, Modification date: 2016/01/14

Ports

tcp/445

18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that may allow an attacker to execute arbitrary code on the remote host.

An attacker does not need to be authenticated to exploit this flaw.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms05-027

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	13942
CVE	CVE-2005-1206
XREF	OSVDB:17308
XREF	MSFT:MS05-027

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2005/06/16, Modification date: 2013/11/04

Ports

tcp/445

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check) [-/+]

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System'
privileges.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	31874
CVE	CVE-2008-4250
XREF	OSVDB:49243
XREF	MSFT:MS08-067
XREF	CERT:827267
XREF	IAVA:2008-A-0081
XREF	EDB-ID:6824
XREF	EDB-ID:7104
XREF	EDB-ID:7132
XREF	CWE:94

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2008/10/23, Modification date: 2016/05/19

Ports

tcp/445

11808 - MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote version of Windows contains a flaw in the function RemoteActivation() in its RPC interface that could allow an attacker to execute arbitrary code on the remote host with the SYSTEM privileges.

A series of worms (Blaster) are known to exploit this vulnerability in the wild.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms03-026

Solution

Microsoft has released patches for Windows NT, 2000, XP, and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	8205
CVE	CVE-2003-0352
XREF	OSVDB:2100
XREF	MSFT:MS03-026

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2003/07/28, Modification date: 2014/07/11

Ports

tcp/445

21696 - MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280) (uncredentialed check) [-/+]

Synopsis

It is possible to execute code on the remote host.

Description

The remote version of Windows contains a version of RRAS (Routing and Remote Access Service) that is affected by several memory corruption vulnerabilities.

An attacker may exploit these flaws to execute code on the remote service.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms06-025

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	18325
BID	18358
CVE	CVE-2006-2370
CVE	CVE-2006-2371
XREF	OSVDB:26436
XREF	OSVDB:26437
XREF	MSFT:MS06-025

Exploitable with

CANVAS (true)Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2006/06/13, Modification date: 2015/05/22

Ports

tcp/445

22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to heap overflow in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with 'SYSTEM' privileges.

In addition to this, the remote host is also affected by an information disclosure vulnerability in SMB that may allow an attacker to obtain portions of the memory of the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms06-035
https://www.tenable.com/security/research/tra-2006-01

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	18863
BID	18891
CVE	CVE-2006-1314
CVE	CVE-2006-1315
XREF	OSVDB:27154
XREF	OSVDB:27155
XREF	TRA:TRA-2006-01
XREF	MSFT:MS06-035

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2006/07/12, Modification date: 2015/10/07

Ports

tcp/445

42411 - Microsoft Windows SMB Shares Unprivileged Access [-/+]

Synopsis

It is possible to access a network share.

Description

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.

Solution

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

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

7.5 (CVSS2#E:H/RL:U/RC:ND)

References

BID	8026
CVE	CVE-1999-0519
CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Publication date: 2009/11/06, Modification date: 2011/03/27

Ports

tcp/445

The following shares can be accessed as iivtbmoh :

- SharedDocs - (readable)
+ Content of this share :
..
desktop.ini
Immagini
Musica

11110 - MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION Packet Remote Overflow DoS (326830) (uncredentialed check) [-/+]

Synopsis

The remote host is vulnerable to a denial of service attack.

Description

The remote host is vulnerable to a denial of service attack in its SMB stack.

An attacker may exploit this flaw to crash the remote host remotely, without any authentication.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms02-045

Solution

Apply the appropriate patches from MS02-045 or apply the latest Windows service pack.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	5556
CVE	CVE-2002-0724
XREF	OSVDB:2074
XREF	MSFT:MS02-045

Plugin Information:

Publication date: 2002/08/23, Modification date: 2016/05/26

Ports

tcp/445

26920 - Microsoft Windows SMB NULL Session Authentication [-/+]

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

http://support.microsoft.com/kb/q143474/
http://support.microsoft.com/kb/q246261/
http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\
restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\
parameters\NullSessionPipes

Reboot once the registry changes are complete.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.2 (CVSS2#E:U/RL:U/RC:ND)

References

BID	494
CVE	CVE-1999-0519
CVE	CVE-1999-0520
CVE	CVE-2002-1117
XREF	OSVDB:299
XREF	OSVDB:8230

Plugin Information:

Publication date: 2007/10/04, Modification date: 2012/02/29

Ports

tcp/445

It was possible to bind to the \browser pipe

20928 - MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (911927) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote version of Windows contains a flaw in the Web Client service that may allow an attacker to execute arbitrary code on the remote host.

To exploit this flaw, an attacker would need credentials to log into the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms06-008

Solution

Microsoft has released a set of patches for Windows XP and 2003.

Risk Factor

Medium

CVSS Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSS Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	16636
CVE	CVE-2006-0013
XREF	OSVDB:23134
XREF	MSFT:MS06-008

Plugin Information:

Publication date: 2006/02/15, Modification date: 2013/11/04

Ports

tcp/445

26919 - Microsoft Windows SMB Guest Account Local User Access [-/+]

Synopsis

It is possible to log into the remote host.

Description

The remote host is running one of the Microsoft Windows operating systems or the SAMBA daemon. It was possible to log into it as a guest user using a random account.

Solution

In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'. Disable the Guest account if applicable.

If the SAMBA daemon is running, double-check the SAMBA configuration around guest user access and disable guest access if appropriate

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0505
XREF	OSVDB:3106

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 2007/10/04, Modification date: 2016/04/05

Ports

tcp/445

16337 - MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302) (uncredentialed check) [-/+]

Synopsis

System information about the remote host can be obtained by an anonymous user.

Description

The remote version of Windows contains a flaw that may allow an attacker to cause it to disclose information over the use of a named pipe through a NULL session.

An attacker may exploit this flaw to gain more knowledge about the remote host.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms05-007

Solution

Microsoft has released a set of patches for Windows XP.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	12486
CVE	CVE-2005-0051
XREF	OSVDB:13596
XREF	MSFT:MS05-007

Plugin Information:

Publication date: 2005/02/10, Modification date: 2015/01/12

Ports

tcp/445

11011 - Microsoft Windows SMB Service Detection [-/+]

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

A CIFS server is running on this port.

10736 - DCE Services Enumeration [-/+]

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\msgsvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe

Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \pipe\keysvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\SECLOGON
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\AudioSrv
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000

UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\PC-VITTIMA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\PC-VITTIMA

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

Synopsis

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

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2016/01/13

Ports

tcp/445

The remote Operating System is : Windows 5.1

The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : PC-VITTIMA

10394 - Microsoft Windows SMB Log In Possible [-/+]

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Supplied credentials

See Also

http://support.microsoft.com/kb/143474
http://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2016/03/11

Ports

tcp/445

- NULL sessions are enabled on the remote host.
- Remote users are authenticated as 'Guest'.

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/445

Port 445/tcp was found to be open

10395 - Microsoft Windows SMB Shares Enumeration [-/+]

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

Here are the SMB shares available on the remote host when logged in as iivtbmoh:

- IPC$
- SharedDocs
- ADMIN$
- C$

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration [-/+]

Synopsis

It is possible to obtain the host SID for the remote host.

Description

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

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

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

The remote host SID value is :

1-5-21-842925246-162531612-682003330

The value of 'RestrictAnonymous' setting is : unknown

10860 - SMB Use Host SID to Enumerate Local Users [-/+]

Synopsis

It is possible to enumerate local users.

Description

Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:714

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- HelpAssistant (id 1000)
- HelpServicesGroup (id 1001)
- SUPPORT_388945a0 (id 1002)
- georgia (id 1003)
- Gigi (id 1004)
- james (id 1005)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry [-/+]

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

Could not connect to the registry because:
Could not connect to \winreg

1025/tcp

13852 - MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check) [-/+]

Synopsis

Arbitrary code can be executed on the remote host.

Description

There is a flaw in the Task Scheduler application which could allow a remote attacker to execute code remotely. There are many attack vectors for this flaw. An attacker, exploiting this flaw, would need to either have the ability to connect to the target machine or be able to coerce a local user to either install a .job file or browse to a malicious website.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms04-022

Solution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

Risk Factor

Critical

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	10708
CVE	CVE-2004-0212
XREF	OSVDB:7798
XREF	MSFT:MS04-022

Plugin Information:

Publication date: 2004/07/29, Modification date: 2014/07/11

Ports

tcp/1025

10736 - DCE Services Enumeration [-/+]

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind

to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/1025

The following DCERPC services are available on TCP port 1025 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 1025
IP : 192.168.15.120

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 1025
IP : 192.168.15.120

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 1025
IP : 192.168.15.120

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0

Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
TCP Port : 1025
IP : 192.168.15.120

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/1025

Port 1025/tcp was found to be open

1026/udp

10736 - DCE Services Enumeration [-/+]

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

udp/1026

The following DCERPC services are available on UDP port 1026 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc, version 1.0
Description : Messenger Service
Windows process : svchost.exe
Annotation : Messenger Service
Type : Remote RPC service
UDP Port : 1026
IP : 192.168.15.120

1900/udp

10829 - UPnP Client Detection [-/+]

Synopsis

This machine is a UPnP client.

Description

This machine answered to a unicast UPnP NOTIFY packet by trying to fetch the XML description that Nessus advertised.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/12/29, Modification date: 2014/05/09

Ports

udp/1900

3306/tcp

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/3306

Port 3306/tcp was found to be open

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/3306

A MySQL server is running on this port.

5000/tcp

11219 - Nessus SYN scanner [-/+]

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2014/01/23

Ports

tcp/5000

Port 5000/tcp was found to be open

11765 - UPnP TCP Helper Detection [-/+]

Synopsis

The remote host appears to be running Microsoft UPnP TCP helper.

Description

The remote host is running Microsoft UPnP TCP helper.

If the tested network is not a home network, you should disable this service.

Solution

Set the following registry key :
Location : HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV Key : Start
Value : 0x04

Risk Factor

None

Plugin Information:

Publication date: 2003/06/19, Modification date: 2011/03/11

Ports

tcp/5000

22964 - Service Detection [-/+]

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/03/17

Ports

tcp/5000

A web server is running on this port.

Remediations

[-] Collapse All
[+] Expand All

Suggested Remediations

Taking the following actions across 1 hosts would resolve 42% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities: Upgrade to PHP version 5.3.29 or later.	97	1
OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS: Upgrade to OpenSSL version 0.9.8zh or later.	47	1
Apache 2.2.x < 2.2.28 Multiple Vulnerabilities: Upgrade to Apache version 2.2.29 or later. Note that version 2.2.28 was never officially released.	35	1
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check): Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.	5	1
MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280) (uncredentialed check): Microsoft has released a set of patches for Windows 2000, XP and 2003.	2	1