



List of hosts

192.168.1.100

High Severity problem(s) found

[\[^\] Back](#)

192.168.1.100

Scan time :

Start time : Sat Oct 31 14:56:26 2009
End time : Sat Oct 31 15:02:53 2009

Number of vulnerabilities :

Open ports : 6
Low : 21
Medium : 8
High : 7

Information about the remote host :

Operating system : Linux Kernel 2.6
NetBIOS name : (unknown)
DNS name : (unknown)

[\[^\] Back to 192.168.1.100](#)

Port smtp (25/tcp)

Service Detection

An SMTP server is running on this port.

Nessus ID : [22964](#)

smtpscan SMTP Fingerprinting

Synopsis :

It is possible to fingerprint the remote mail server.

Description :

smtpscan is a SMTP fingerprinting tool written by Julien Bordet It identifies the remote mail server even if the banners were changed.

Solution :

n/a

Risk factor :

None

Plugin output :

This server could be fingerprinted as :

Sendmail 8.12.3

Nessus ID : [11421](#)

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 output :

Remote SMTP server banner :

220 slax.example.net ESMTP Sendmail 8.13.7/8.13.7; Sat, 31 Oct 2009 14:59:02 GMT

Nessus ID : [10263](#)

[\[^\] Back to 192.168.1.100](#)

Port ftp (21/tcp)

FTP Server Detection

Synopsis :

An FTP server is listening on this port.

Description :

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

Solution :

N/A

Risk factor :

None

Plugin output :

The remote FTP banner is :

500 OOPS: could not bind listening IPv4 socket

Nessus ID : [10092](#)

[\[^\] Back to 192.168.1.100](#)

Port ssh (22/tcp)

Service Detection

An SSH server is running on this port.

Nessus ID : [22964](#)

SSH Server Type and Version Information

Synopsis :

An SSH server is listening on this port.

Description :

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Risk factor :

None

Plugin output :

SSH version : SSH-1.99-OpenSSH_4.3

SSH supported authentication : publickey,password,keyboard-interactive

Nessus ID : [10267](#)

SSH Protocol Version 1 Session Key Retrieval

Synopsis :

The remote service offers an insecure cryptographic protocol.

Description :

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

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

Solution :

Disable compatibility with version 1 of the protocol.

Risk factor :

Medium / CVSS Base Score : 4.0
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)

CVE : CVE-2001-0361

BID : 2344

Other references : OSVDB:2116

Nessus ID : [10882](#)

SSH Protocol Versions Supported

Synopsis :

A SSH server is running on the remote host.

Description :

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution :

n/a

Risk factor :

None

Plugin output :

The remote SSH daemon supports the following versions of the SSH protocol :

- 1.33
- 1.5
- 1.99
- 2.0

SSHv1 host key fingerprint : 4d:5c:f8:56:95:2a:6f:2b:c5:16:4e:53:27:73:ec:fc
SSHv2 host key fingerprint : ab:ab:a8:ad:a2:f2:fd:c2:6f:05:99:69:40:54:ec:10

Nessus ID : [10881](#)

Backported Security Patch Detection (SSH)

Synopsis :

Security patches are backported.

Description :

Security patches may have been 'back ported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See also :

<http://www.nessus.org/u?d636c8c7>

Solution :

N/A

Risk factor :

None

Plugin output :

Give Nessus credentials to perform local checks.

Nessus ID : [39520](#)

[\[<\] Back to 192.168.1.100](#)

Port general/udp

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 output :

For your information, here is the traceroute from 192.168.1.2 to 192.168.1.100 :
192.168.1.2
192.168.1.100

Nessus ID : [10287](#)

[\[<\] Back to 192.168.1.100](#)

Port pop3 (110/tcp)

Service Detection

A POP3 server is running on this port.

Nessus ID : [22964](#)

[\[<\] Back to 192.168.1.100](#)

Port general/tcp

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>

Risk factor :

None

Nessus ID : [25220](#)

Ethernet card brand

Synopsis :

The manufacturer can be deduced from the Ethernet OUI.

Description :

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

See also :

<http://standards.ieee.org/faqs/OUI.html>
<http://standards.ieee.org/regauth/oui/index.shtml>

Risk factor :

None

Plugin output :

The following card manufacturers were identified :

00:0c:29:2b:ed:af : VMware, Inc.

Nessus ID : [35716](#)

VMware Virtual Machine Detection

Synopsis :

The remote host seems to be a VMware virtual machine.

Description :

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

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk factor :

None

Nessus ID : [20094](#)

OS Identification

Remote operating system : Linux Kernel 2.6
Confidence Level : 70
Method : SinFP

The remote host is running Linux Kernel 2.6

Nessus ID : [11936](#)

Nessus Scan Information

Information about this scan :

Nessus version : 4.0.2 (Build 1076)
Plugin feed version : 200910310134
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.1.2
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : yes
Experimental tests : yes
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
CGI scanning : enabled
Web application tests : disabled
Max hosts : 40
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2009/10/31 14:56
Scan duration : 387 sec

Nessus ID : [19506](#)

[\[^\] Back to 192.168.1.100](#)

Port http (80/tcp)

Service Detection

A web server is running on this port.

Nessus ID : [22964](#)

Web Server Directory Enumeration

Synopsis :

It is possible to enumerate directories on the web server.

Description :

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Risk factor :

None

Plugin output :

The following directories were discovered:
/cgi-bin, /icons

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Other references : OWASP:OWASP-CM-006

Nessus ID : [11032](#)

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.

Risk factor :

None

Plugin output :

The remote web server type is :

Apache/2.0.55 (Unix) PHP/5.1.2

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

Nessus ID : [10107](#)

PHP < 5.2.5 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 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows.

See also :

http://www.php.net/releases/5_2_5.php

Solution :

Upgrade to PHP version 5.2.5 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2007-4887, CVE-2007-5898, CVE-2007-5900
BID : 26403

Other references : OSVDB:38680, OSVDB:38681, OSVDB:38682, OSVDB:38683, OSVDB:38684, OSVDB:38685

Nessus ID : [28181](#)

PHP < 5.2.6 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

According to its banner, the version of PHP installed on the remote host is older than 5.2.6. Such versions may be affected by the following issues :

- A stack buffer overflow in FastCGI SAPI.
- An integer overflow in printf().
- A security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c.
- A safe_mode bypass in cURL.
- Incomplete handling of multibyte chars inside escapeshellcmd().
- Issues in the bundled PCRE fixed by version 7.6.

See also :

<http://archives.neohapsis.com/archives/bugtraq/2008-03/0321.html>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0103.html>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-05/0107.html>
http://www.php.net/releases/5_2_6.php

Solution :

Upgrade to PHP version 5.2.6 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2007-4850, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051
BID : 27413, 28392, 29009

Other references : OSVDB:43219, OSVDB:44057, OSVDB:44906, OSVDB:44907, OSVDB:44908, Secunia:30048

Nessus ID : [32123](#)

PHP < 5.2.11 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 is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.
- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.
- An unspecified input validation vulnerability affects exif processing.
- A denial-of-service issue relates to 'popen' when invalid modes are passed.

See also :

http://www.php.net/releases/5_2_11.php
<http://news.php.net/php.internals/45597>
<http://www.php.net/ChangeLog-5.php#5.2.11>

Solution :

Upgrade to PHP version 5.2.11 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

BID : 36449
Other references : Secunia:36791

Nessus ID : [41014](#)

PHP < 5.2.3 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 installed on the remote host is older than 5.2.3. Such versions may be affected by several issues, including an integer overflow, 'safe_mode' and 'open_basedir' bypass, and a denial of service vulnerability.

See also :

http://www.php.net/releases/5_2_3.php

Solution :

Upgrade to PHP version 5.2.3 or later.

Risk factor :

Medium / CVSS Base Score : 6.9
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007
BID : 23359, 24089, 24259, 24261

Other references : OSVDB:33962, OSVDB:35788, OSVDB:36083, OSVDB:36084, OSVDB:36643

Nessus ID : [25368](#)

PHP < 5.2 Multiple Vulnerabilities

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows.

To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server, or to be able to manipulate several variables processed by some PHP functions such as htmlentities().

See also :

http://www.php.net/releases/5_2_0.php

Solution :

Upgrade to PHP version 5.2.0 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2006-5465
BID : 20879

Other references : OSVDB:30178, OSVDB:30179

Nessus ID : [31649](#)

Apache < 2.0.63 Multiple XSS Vulnerabilities

Synopsis :

The remote web server may be affected by several issues.

Description :

According to its banner, the version of Apache 2.0 installed on the remote host is older than 2.0.63. Such versions may be affected by several issues, including :

- A cross-site scripting issue involving mod_imap.
(CVE-2007-5000)

- A cross-site scripting issue involving 413 error pages via a malformed HTTP method. (PR 44014 / CVE-2007-6203)

- A cross-site scripting issue in mod_status involving the refresh parameter. (CVE-2007-6388)

- A cross-site scripting issue using UTF-7 encoding in mod_proxy_ftp exists because it does not define a charset. (CVE-2008-0005)

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://www.apache.org/dist/httpd/CHANGES_2.0.63

http://httpd.apache.org/security/vulnerabilities_20.html

Solution :

Either ensure that the affected modules are not in use or upgrade to Apache version 2.0.63 or later.

Risk factor :

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

Plugin output :

According to its banner, Apache version 2.0.55 is installed on the remote host.

CVE : CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2008-0005
BID : 26663, 26838, 27234, 27237
Other references : OSVDB:39003, OSVDB:39134, OSVDB:40262, OSVDB:42214

Nessus ID : 3140Z

PHP 5 < 5.2.7 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 5.2.7. Such versions may be affected by several security issues :

- File truncation can occur when calling 'dba_replace()' with an invalid argument.
- There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371)
- A buffer overflow in the 'imagerloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)
- There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659)
- When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg, 'file..php'). (CVE-2008-3660)
- Multiple directory traversal vulnerabilities in functions such as 'posix_access()', 'chdir()', 'ftok()' may allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666).
- A buffer overflow may be triggered when processing long message headers in 'php_imap.c' due to use of an obsolete API call. (CVE-2008-2829)
- A heap-based buffer overflow may be triggered via a call to 'mb_check_encoding()', part of the 'mbstring' extension. (CVE-2008-5557)
- Missing initialization of 'BG(page_uid)' and 'BG(page_gid)' when PHP is used as an Apache module may allow for bypassing security restriction due to SAPI 'php_getuid()' overloading. (CVE-2008-5624)
- Incorrect 'php_value' order for Apache configuration may allow bypassing PHP's 'safe_mode' setting. (CVE-2008-5625)
- The ZipArchive::extractTo() method in the ZipArchive extension fails to filter directory traversal sequences from file names. (CVE-2008-5658)

See also :

http://securityreason.com/achievement_securityalert/57
http://securityreason.com/achievement_securityalert/58
http://securityreason.com/achievement_securityalert/59
<http://www.sektioneins.de/advisories/SE-2008-06.txt>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-06/0238.html>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-06/0239.html>
<http://www.openwall.com/lists/oss-security/2008/08/08/2>
<http://www.openwall.com/lists/oss-security/2008/08/13/8>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-11/0433.html>
<http://archives.neohapsis.com/archives/fulldisclosure/2008-12/0089.html>
<http://bugs.php.net/bug.php?id=42862>
<http://bugs.php.net/bug.php?id=45151>
<http://bugs.php.net/bug.php?id=45722>
http://www.php.net/releases/5_2_7.php
<http://www.php.net/ChangeLog-5.php#5.2.7>

Solution :

Upgrade to PHP version 5.2.8 or later.

Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658

BID : 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948

Other references : OSVDB:46584, OSVDB:46638, OSVDB:46639, OSVDB:46641, OSVDB:46690, OSVDB:47796, OSVDB:47797, OSVDB:47798, OSVDB:50480, OSVDB:51477, OSVDB:52205, OSVDB:52206, OSVDB:52207

Nessus ID : [35043](#)

PHP < 5.2.4 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 installed on the remote host is older than 5.2.4. Such versions may be affected by various issues, including but not limited to several overflows.

See also :

http://www.php.net/releases/5_2_4.php

Solution :

Upgrade to PHP version 5.2.4 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2007-2872, CVE-2007-3378, CVE-2007-3806

BID : 24661, 24261, 24922, 25498

Other references : OSVDB:36083, OSVDB:36085, OSVDB:36869

Nessus ID : [25971](#)

Web Server info.php / phpinfo.php Detection

Synopsis :

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description :

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed php and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution :

Remove the affected file(s).

Risk factor :

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

Plugin output :

Nessus discovered the following URL that calls phpinfo() :

- <http://192.168.1.100/info.php>

Nessus ID : [11229](#)

PHP < 5.2.1 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 installed on the remote host is older than 5.2.1. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.

See also :

http://www.php.net/releases/5_2_1.php

Solution :

Upgrade to PHP version 5.2.1 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, CVE-2007-0909, CVE-2007-0910, CVE-2007-1376, CVE-2007-1380, CVE-2007-1453, CVE-2007-1700, CVE-2007-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1890

BID : 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, 23235, 23236, 23237, 23238

Other references : OSVDB:32763, OSVDB:32764, OSVDB:32765, OSVDB:32766, OSVDB:32767, OSVDB:32768, OSVDB:32776, OSVDB:32781, OSVDB:33269, OSVDB:33933, OSVDB:33944, OSVDB:33945, OSVDB:33955, OSVDB:33957, OSVDB:33958, OSVDB:33959, OSVDB:33960, OSVDB:34767

Nessus ID : [24907](#)

PHP < 5.2.10 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 older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)

- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

See also :

<http://bugs.php.net/bug.php?id=45997>

<http://bugs.php.net/bug.php?id=48378>

http://www.php.net/releases/5_2_10.php

<http://www.php.net/Changelog-5.php#5.2.10>

Solution :

Upgrade to PHP version 5.2.10 or later.

Risk factor :

Medium / CVSS Base Score : 5.2
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

Server: Apache/2.0.55 (Unix) PHP/5.1.2

CVE : CVE-2009-2687

BID : 35440, 35435

Other references : OSVDB:55222, OSVDB:55223, OSVDB:55224, Secunia:35441

Nessus ID : [39480](#)

Apache < 2.0.59 mod_rewrite LDAP Protocol URL Handling Overflow

Synopsis :

The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.

Description :

The remote host appears to be running a version of Apache which is older than 2.0.59.

This version contains an off-by-one buffer overflow in the mod_rewrite

This plugin contains an error by the server version in the mod_rewrite module.

See also :

<http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/048265.html>
http://www.apache.org/dist/httpd/CHANGES_2.0
<http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/048269.html>

Solution :

Upgrade to version 2.0.59 or later.

Risk factor :

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

Plugin output :

According to its banner, Apache version 2.0.55 is installed on the remote host.

CVE : CVE-2006-3747
BID : 19204
Other references : OSVDB:27588

Nessus ID : 31655

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.

Risk factor :

None

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : yes
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Sat, 31 Oct 2009 15:01:40 GMT
Server: Apache/2.0.55 (Unix) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Content-Length: 1983
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Nessus ID : 24260

HTTP TRACE / TRACK Methods Allowed

Synopsis :

Debugging functions are enabled on the remote web server.

Description :

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

In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

See also :

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
<http://www.apacheweek.com/issues/03-01-24>
<http://www.kb.cert.org/vuls/id/288308>
<http://www.kb.cert.org/vuls/id/867593>

Solution :

Disable these methods.

Risk factor :

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

Solution :

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.

Plugin output :

Nessus sent the following TRACE request :

```
----- snip -----
TRACE /Nessus32226.html HTTP/1.1
Connection: Close
Host: 192.168.1.100
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

and received the following response from the remote server :

```
----- snip -----
HTTP/1.1 200 OK
Date: Sat, 31 Oct 2009 15:01:42 GMT
Server: Apache/2.0.55 (Unix) PHP/5.1.2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus32226.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.1.100
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
----- snip -----
CVE : CVE-2003-1567, CVE-2004-2320
BID : 9506, 9561, 11604, 33374
Other references : OSVDB:877, OSVDB:3726, OSVDB:5648, OSVDB:50485
```

Nessus ID : 11213

PHP < 5.2.9 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 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)
- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.
- Function 'explode()' is affected by an unspecified vulnerability.
- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.
- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See also :

- <http://news.php.net/php.internals/42762>
- http://www.php.net/releases/5_2_9.php
- <http://www.php.net/ChangeLog-5.php#5.2.9>

Solution :

Upgrade to PHP version 5.2.9 or later.

Risk factor :

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

Plugin output :

PHP version 5.1.2 appears to be running on the remote host based on the following Server response header :

```
Server: Apache/2.0.55 (Unix) PHP/5.1.2
CVE : CVE-2008-5498
BID : 33002, 33927
Other references : OSVDB:51031, Secunia:34081
```

Nessus ID : 35750

Port imap (143/tcp)
Service Detection
An IMAP server is running on this port. Nessus ID : 22964
IMAP Service Banner Retrieval
Synopsis : An IMAP server is running on the remote host.
Description : An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.
Solution : n/a
Risk factor : None
Plugin output : The remote imap server banner is : * OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS AUTH=LOGIN] [192.168.1.100] IMAP4rev1 2004.357 at Sat, 31 Oct 2009 14:59:01 +0000 (GMT)
Nessus ID : 11414