Summary

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

Scan started at: Mon Oct 11 16:08:20 2021
Scan finished at: Mon Oct 11 16:23:40 2021

Host	Possible Issues	Holes	Warnings	Notes	False Positives
alice	Security hole(s) found	5	15	41	0
Total: 1		5	15	41	0

Reports per Host

alice

Scan of this host started at: Mon Oct 11 16:08:20 2021
Scan of this host finished at: Mon Oct 11 16:23:40 2021

Service (Port)	Issue regarding port
ftp (21/tcp)	Security hole(s) found
ssh (22/tcp)	Security note(s) found
telnet (23/tcp)	Security note(s) found
smtp (25/tcp)	Security note(s) found
http (80/tcp)	Security hole(s) found
sunrpc (111/tcp)	Security note(s) found
https (443/tcp)	Security warning(s) found
nfs (2049/tcp)	Security note(s) found
x11 (6000/tcp)	Security note(s) found
unknown (961/tcp)	Security note(s) found
unknown (38964/tcp)	Security note(s) found
unknown (55068/tcp)	Security note(s) found
unknown (57583/tcp)	Security note(s) found
sunrpc (111/udp)	Security note(s) found
unknown (960/udp)	Security note(s) found
nfs (2049/udp)	Security note(s) found
unknown (40009/udp)	Security note(s) found
unknown (42046/udp)	Security note(s) found
unknown (49650/udp)	Security note(s) found
general/tcp	Security note(s) found
general/SMBClient	No Information
ntp (123/udp)	Security note(s) found
general/IT-Grundschutz	No Information

general/icmp	Security note(s) found
general/IT-Grundschutz-T	No Information
general/CPE-T	No Information

[return to summary]

Security Issues and Fixes - Host alice

alice - ftp (21/tcp)

Vulnerability

The remote Wu-FTPd server seems to be vulnerable to a remote flaw.

This version fails to properly check bounds on a pathname when Wu-Ftpd is
compiled with MAIL_ADMIN enabled resulting in a buffer overflow. With a
specially crafted request, an attacker can possibly execute arbitrary code
as the user Wu-Ftpd runs as (usually root) resulting in a loss of integrity,
and/or availability.

It should be noted that this vulnerability is not present within the default
installation of Wu-Ftpd.

The server must be configured using the 'MAIL_ADMIN' option to notify an
administrator when a file has been uploaded.

*** OpenVAS solely relied on the banner of the remote server
*** to issue this warning, so it may be a false positive.

Solution : Upgrade to Wu-FTPd 2.6.3 when available
Risk factor : High
CVE : CVE-2003-1327
BID : 8668
Other references : OSVDB:2594
OID : 1.3.6.1.4.1.25623.1.0.14371

Vulnerability

The remote Wu-FTPd server seems to be vulnerable to a remote overflow.

This version contains a remote overflow if s/key support is enabled.
The skey_challenge function fails to perform bounds checking on the
name variable resulting in a buffer overflow.
With a specially crafted request, an attacker can execute arbitrary
code resulting in a loss of integrity and/or availability.

It appears that this vulnerability may be exploited prior to authentication.
It is reported that S/Key support is not enabled by default,
though some operating system distributions which ship Wu-Ftpd may have it
enabled.

*** OpenVAS solely relied on the banner of the remote server
*** to issue this warning, so it may be a false positive.

Solution : Upgrade to Wu-FTPd 2.6.3 when available or disable SKEY or apply the patches available at http://www.wu-ftpd.org

Risk factor : High
CVE : CVE-2004-0185
BID : 8893
Other references : OSVDB:2715, RHSA:RHSA-2004:096-09, DSA:DSA-457-1
OID : 1.3.6.1.4.1.25623.1.0.14372

Informational
An FTP server is running on this port. Here is its banner : 220 alice FTP server (Version wu-2.6.2(1) Wed Sep 30 08:44:57 UTC 2009) ready. OID : 1.3.6.1.4.1.25623.1.0.10330
Informational
Remote FTP server banner : 220 alice FTP server (Version wu-2.6.2(1) Wed Sep 30 08:44:57 UTC 2009) ready. OID : 1.3.6.1.4.1.25623.1.0.10092

[return to alice]

alice - ssh (22/tcp)

Informational
An ssh server is running on this port OID : 1.3.6.1.4.1.25623.1.0.10330
Informational
Remote SSH version : SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu5 Remote SSH supported authentication : publickey,password OID : 1.3.6.1.4.1.25623.1.0.10267
Informational
Overview: The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 Risk factor : None OID : 1.3.6.1.4.1.25623.1.0.100259

[return to alice]

alice - telnet (23/tcp)

Informational
A telnet server seems to be running on this port OID : 1.3.6.1.4.1.25623.1.0.10330
Informational
Overview: A telnet Server is running at this host. Experts in computer security, such as SANS Institute, and the members of the comp.os.linux.security newsgroup recommend that the use of Telnet for remote logins should be discontinued under all normal circumstances, for the following reasons: * Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes; anybody who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login and password information (and whatever else is typed) with any of several common utilities like tcpdump and Wireshark. * Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle. * Commonly used Telnet daemons have several vulnerabilities discovered over the years. Risk factor : Medium OID : 1.3.6.1.4.1.25623.1.0.100074
Informational
Remote telnet banner : Ubuntu 10.04.2 LTS alice login: OID : 1.3.6.1.4.1.25623.1.0.10281

[return to alice]

alice - smtp (25/tcp)

Informational
An SMTP server is running on this port Here is its banner : 220 alice ESMTP Postfix (Ubuntu) OID : 1.3.6.1.4.1.25623.1.0.10330
Informational
Remote SMTP server banner : 220 alice ESMTP Postfix (Ubuntu)

This is probably: Postfix
OID : 1.3.6.1.4.1.25623.1.0.10263

Informational

Some antivirus scanners dies when they process an email with a
too long string without line breaks.
Such a message was sent. If there is an antivirus on your MTA,
it might have crashed. Please check its status right now, as
it is not possible to do it remotely

OID : 1.3.6.1.4.1.25623.1.0.11270

Informational

The file 42.zip was sent 2 times. If there is an antivirus in your MTA, it might
have crashed. Please check its status right now, as it is
not possible to do so remotely

BID : 3027
OID : 1.3.6.1.4.1.25623.1.0.11036

[return to alice]

alice - http (80/tcp)

Vulnerability

Overview:
PHP is prone to a vulnerability that an attacker could exploit to
execute arbitrary code with the privileges of the user running the
affected application. Successful exploits will compromise the
application and possibly the computer.

References:
https://www.securityfocus.com/bid/40948
https://bugzilla.redhat.com/show_bug.cgi?id=605641
http://www.php.net
BID : 40948
OID : 1.3.6.1.4.1.25623.1.0.100684

Vulnerability

Overview:
PHP is prone to multiple vulnerabilities that may allow
attackers to execute arbitrary code.

Attackers can exploit these issues to run arbitrary code within the
context of the PHP process. This may allow them to bypass intended
security restrictions or gain elevated privileges.

References:
http://www.securityfocus.com/bid/40013
http://php-security.org/2010/05/07/mops-2010-012-php-sqlite_single_query-uninitialized-memory-usage-vulnerability/index.html
http://php-security.org/2010/05/07/mops-2010-013-php-sqlite_array_query-uninitialized-memory-usage-vulnerability/index.html
http://www.php.net

http://php-security.org/2010/05/07/mops-submission-03-sqlite_single_query-sqlite_array_query-uninitialized-memory-usage/inde
BID : 40013
OID : 1.3.6.1.4.1.25623.1.0.100631

Vulnerability

Overview:
PHP is prone to multiple format-string vulnerabilities because it fails to properly sanitize user-supplied input before passing it as the format specifier to a formatted-printing function.

Attackers can exploit these issues to run arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges.

PHP 5.3 through 5.3.2 are vulnerable.

Solution:
Updates are available; please see the references for details.

References:
http://www.securityfocus.com/bid/40173
http://www.mail-archive.com/php-cvs@lists.php.net/msg46330.html
http://svn.php.net/viewvc?view=revision&revision=298667
http://php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-025-php-phar_wrapper_open_dir-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-026-php-phar_wrapper_unlink-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-027-php-phar_parse_url-format-string-vulnerabilities/index.html
http://php-security.org/2010/05/14/mops-2010-028-php-phar_wrapper_open_url-format-string-vulnerabilities/index.html
http://www.php.net
BID : 40173
OID : 1.3.6.1.4.1.25623.1.0.100643

Warning

The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker :
/phpinfo.php

Solution : Delete them or restrict access to them
Risk factor : Low
OID : 1.3.6.1.4.1.25623.1.0.11229

Warning

Overview:

phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability.

These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also

possible.

Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/34253

Risk factor : Medium
BID : 34253
OID : 1.3.6.1.4.1.25623.1.0.100078

Warning

Overview: This host is running PHP and is prone to multiple information
disclosure vulnerabilities.

Vulnerability Insight:
Multiple flaws are due to:
- Error in 'trim()', 'ltrim()','rtrim()' and 'substr_replace()' functions,
which causes a userspace interruption of an internal function within the
call time pass by reference feature.
- Error in 'parse_str()', 'preg_match()', 'unpack()' and 'pack()' functions,
'ZEND_FETCH_RW()', 'ZEND_CONCAT()', and 'ZEND_ASSIGN_CONCAT()' opcodes, and
the 'ArrayObject::uasort' method, trigger memory corruption by causing a
userspace interruption of an internal function or handler.

Impact:
Successful exploitation could allow local attackers to bypass certain security
restrictions and to obtain sensitive information.

Impact Level: Network

Affected Software/OS:
PHP version 5.2 through 5.2.13 and 5.3 through 5.3.2

Fix: No solution or patch is available as on 11th June, 2010. Information
regarding this issue will be updated once the solution details are available.
For updates refer, http://www.php.net/downloads.php

References:
http://www.php-security.org/2010/05/30/mops-2010-048-php-substr_replace-interruption-information-leak-vulnerability/index.htr
http://www.php-security.org/2010/05/30/mops-2010-047-php-trimltrimrtrim-interruption-information-leak-vulnerability/index.htn
CVE : CVE-2010-2190, CVE-2010-2191
OID : 1.3.6.1.4.1.25623.1.0.801359

Warning

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities,
including an HTML-injection vulnerability, cross-site
scripting vulnerabilities, and information-disclosure

vulnerabilities.

An attacker could exploit these vulnerabilities to view sensitive
information or to have arbitrary script code execute in the context
of the affected site, which may allow the attacker to steal
cookie-based authentication credentials or change the way the site
is rendered to the user. Data gained could aid in further attacks.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/21137

Risk factor : Medium
CVE : CVE-2006-6942
BID : 21137
OID : 1.3.6.1.4.1.25623.1.0.100068

Warning

Overview:
PHP is prone to a remote integer-overflow vulnerability.

An attacker can exploit this issue to execute arbitrary code in the
context of the PHP process. Failed exploit attempts will result in a
denial-of-service condition.

PHP 5.3.0 through 5.3.2 are vulnerable; other versions may also
be affected.

References:
http://www.securityfocus.com/bid/39877
http://php-security.org/2010/05/02/mops-2010-003-php-dechunk-filter-signed-comparison-vulnerability/index.html
http://www.php.net
BID : 39877
OID : 1.3.6.1.4.1.25623.1.0.100617

Warning

Overview:
This host is running Apache HTTP Server and is prone to Denial of Service
vulnerability.

Vulnerability Insight:
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c'
in the mod_proxy module. When a reverse proxy is configured, it does not properly
handle an amount of streamed data that exceeds the Content-Length value via
crafted requests.

Impact:
Successful exploitation will allow remote attackers to cause Denial of Service
to the legitimate user by CPU consumption.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server version prior to 2.3.3

Fix:
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=790587

References:
http://secunia.com/advisories/35691
http://www.vupen.com/english/advisories/2009/1773
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.7
Risk factor : Medium
CVE : CVE-2009-1890
BID : 35565
OID : 1.3.6.1.4.1.25623.1.0.800827

Warning

Overview:
Apache is prone to multiple vulnerabilities.

These issues may lead to information disclosure or other attacks.

Apache versions prior to 2.2.15-dev are affected.

Solution:
These issues have been addressed in Apache 2.2.15-dev. Apache 2.2.15
including fixes will become available in the future as well. Please
see the references for more information.

References:
http://www.securityfocus.com/bid/38494
http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://svn.apache.org/viewvc?view=revision&revision=917870

Risk factor : Medium
CVE : CVE-2010-0425, CVE-2010-0434, CVE-2010-0408
BID : 38494, 38491
OID : 1.3.6.1.4.1.25623.1.0.100514

Warning

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities, including a
cross-site scripting and a SQL-injection issue.

A successful exploit may allow an attacker to steal cookie-based
authentication credentials, compromise the application, access or modify data,
or exploit latent vulnerabilities in the underlying database.

These issues affect versions prior to phpMyAdmin 2.11.2.1.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/26512

Risk factor : Medium
CVE : CVE-2007-5976, CVE-2007-5977
BID : 26512
OID : 1.3.6.1.4.1.25623.1.0.100067

Warning

Overview:
The PHP Mysqlnd extension is prone to an information-disclosure
vulnerability and multiple buffer-overflow vulnerabilities.

Successful exploits can allow attackers to obtain sensitive
information or to execute arbitrary code in the context of
applications using the vulnerable PHP functions. Failed attempts may
lead to a denial-of-service condition.

PHP 5.3 through 5.3.2 are vulnerable.

References:
http://www.securityfocus.com/bid/40461
http://php-security.org/2010/05/31/mops-2010-056-php-php_mysqlnd_ok_read-information-leak-vulnerability/index.html
http://php-security.org/2010/05/31/mops-2010-057-php-php_mysqlnd_rset_header_read-buffer-overflow-vulnerability/index.html
http://php-security.org/2010/05/31/mops-2010-058-php-php_mysqlnd_read_error_from_line-buffer-overflow-vulnerability/index.
http://php-security.org/2010/05/31/mops-2010-059-php-php_mysqlnd_auth_write-stack-buffer-overflow-vulnerability/index.html
http://www.php.net/manual/en/book.mysqlnd.php
http://www.php.net/

BID : 40461
OID : 1.3.6.1.4.1.25623.1.0.100662

Warning

The Sambar webserver is running. It provides a web interface for sending emails.
You may simply pass a POST request to /session/sendmail and by this send mails to anyone you want.
Due to the fact that Sambar does not check HTTP referrers you do not need direct access to the server!

Solution : Try to disable this module. There might be a patch in the future.

Risk factor : High
OID : 1.3.6.1.4.1.25623.1.0.10415

Informational

A web server is running on this port
OID : 1.3.6.1.4.1.25623.1.0.10330

Informational

The remote web server type is :

Apache/2.2.14 (Ubuntu)

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

Informational

phpMyAdmin is running at this Host.

phpMyAdmin is a free software tool written in PHP intended to handle
the administration of MySQL over the World Wide Web.

Risk factor : None

phpMyAdmin was detected on the remote host in the following directory(s):

phpMyAdmin (Ver. unknown) under /phpmyadmin.

OID : 1.3.6.1.4.1.25623.1.0.900129

Informational

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

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

The following directories require authentication:
/forum
Other references : OWASP:OWASP-CM-006
OID : 1.3.6.1.4.1.25623.1.0.11032

Informational

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

. (id [forum])

OID : 1.3.6.1.4.1.25623.1.0.10662

[return to alice]

alice - sunrpc (111/tcp)

Informational

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - https (443/tcp)

Warning

Overview:

phpMyAdmin is prone to multiple input-validation vulnerabilities,
including an HTTP response-splitting vulnerability and a
local file-include vulnerability.

These issues can be leveraged to view or execute arbitrary local
scripts, or misrepresent how web content is served, cached, or
interpreted. This could aid in various attacks that try to entice
client users into a false sense of trust. Other attacks are also
possible.

Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/34253

Risk factor : Medium
BID : 34253
OID : 1.3.6.1.4.1.25623.1.0.100078

Warning

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities,
including an HTML-injection vulnerability, cross-site
scripting vulnerabilities, and information-disclosure
vulnerabilities.

An attacker could exploit these vulnerabilities to view sensitive
information or to have arbitrary script code execute in the context
of the affected site, which may allow the attacker to steal
cookie-based authentication credentials or change the way the site
is rendered to the user. Data gained could aid in further attacks.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/21137

Risk factor : Medium
CVE : CVE-2006-6942
BID : 21137

OID : 1.3.6.1.4.1.25623.1.0.100068

Warning

Overview:
This host is running Apache HTTP Server and is prone to Denial of Service vulnerability.

Vulnerability Insight:
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c' in the mod_proxy module. When a reverse proxy is configured, it does not properly handle an amount of streamed data that exceeds the Content-Length value via crafted requests.

Impact:
Successful exploitation will allow remote attackers to cause Denial of Service to the legitimate user by CPU consumption.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server version prior to 2.3.3

Fix:
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=790587

References:
http://secunia.com/advisories/35691
http://www.vupen.com/english/advisories/2009/1773
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.7
Risk factor : Medium
CVE : CVE-2009-1890
BID : 35565
OID : 1.3.6.1.4.1.25623.1.0.800827

Warning

Overview:
Apache is prone to multiple vulnerabilities.

These issues may lead to information disclosure or other attacks.

Apache versions prior to 2.2.15-dev are affected.

Solution:
These issues have been addressed in Apache 2.2.15-dev. Apache 2.2.15 including fixes will become available in the future as well. Please see the references for more information.

References:
http://www.securityfocus.com/bid/38494

http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://svn.apache.org/viewvc?view=revision&revision=917870

Risk factor : Medium
CVE : CVE-2010-0425, CVE-2010-0434, CVE-2010-0408
BID : 38494, 38491
OID : 1.3.6.1.4.1.25623.1.0.100514

Warning

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities, including a
cross-site scripting and a SQL-injection issue.

A successful exploit may allow an attacker to steal cookie-based
authentication credentials, compromise the application, access or modify data,
or exploit latent vulnerabilities in the underlying database.

These issues affect versions prior to phpMyAdmin 2.11.2.1.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/26512

Risk factor : Medium
CVE : CVE-2007-5976, CVE-2007-5977
BID : 26512
OID : 1.3.6.1.4.1.25623.1.0.100067

Informational

A web server is running on this port
OID : 1.3.6.1.4.1.25623.1.0.10330

Informational

The remote web server type is :

Apache/2.2.14 (Ubuntu)

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

Informational

phpMyAdmin is running at this Host.

phpMyAdmin is a free software tool written in PHP intended to handle
the administration of MySQL over the World Wide Web.

Risk factor : None

phpMyAdmin was detected on the remote host in the following directory(s):

phpMyAdmin (Ver. unknown) under /phpmyadmin.

OID : 1.3.6.1.4.1.25623.1.0.900129

Informational

The following directories were discovered:
/icons, /javascript

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
OID : 1.3.6.1.4.1.25623.1.0.11032

[return to alice]

alice - nfs (2049/tcp)

Informational

RPC program #100003 version 2 'nfs' (nfsprog) is running on this port
RPC program #100003 version 3 'nfs' (nfsprog) is running on this port
RPC program #100003 version 4 'nfs' (nfsprog) is running on this port

OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - x11 (6000/tcp)

Informational

This X server does *not* allow any client to connect to it
however it is recommended that you filter incoming connections
to this port as attacker may send garbage data and slow down
your X session or even kill the server.

Here is the server version : 11.0
Here is the message we received : No protocol specified

Solution : filter incoming connections to ports 6000-6009
Risk factor : Low
CVE : CVE-1999-0526
OID : 1.3.6.1.4.1.25623.1.0.10407

[return to alice]

alice - unknown (961/tcp)

Informational
RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port RPC program #100011 version 2 'rquotad' (rquotaprog quota rquota) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (38964/tcp)

Informational
RPC program #100021 version 1 'nlockmgr' is running on this port RPC program #100021 version 3 'nlockmgr' is running on this port RPC program #100021 version 4 'nlockmgr' is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (55068/tcp)

Informational
RPC program #100024 version 1 'status' is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (57583/tcp)

Informational
RPC program #100005 version 1 'mountd' (mount showmount) is running on this port RPC program #100005 version 2 'mountd' (mount showmount) is running on this port RPC program #100005 version 3 'mountd' (mount showmount) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - sunrpc (111/udp)

Informational
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (960/udp)

Informational
RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port RPC program #100011 version 2 'rquotad' (rquotaprog quota rquota) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - nfs (2049/udp)

Informational
RPC program #100003 version 2 'nfs' (nfsprog) is running on this port RPC program #100003 version 3 'nfs' (nfsprog) is running on this port RPC program #100003 version 4 'nfs' (nfsprog) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111
Informational
Here is the export list of alice : /home/alice * CVE : CVE-1999-0554, CVE-1999-0548 OID : 1.3.6.1.4.1.25623.1.0.102014

[return to alice]

alice - unknown (40009/udp)

Informational
RPC program #100021 version 1 'nlockmgr' is running on this port RPC program #100021 version 3 'nlockmgr' is running on this port RPC program #100021 version 4 'nlockmgr' is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (42046/udp)

Informational
RPC program #100005 version 1 'mountd' (mount showmount) is running on this port RPC program #100005 version 2 'mountd' (mount showmount) is running on this port RPC program #100005 version 3 'mountd' (mount showmount) is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - unknown (49650/udp)

Informational
RPC program #100024 version 1 'status' is running on this port OID : 1.3.6.1.4.1.25623.1.0.11111

[return to alice]

alice - general/tcp

Informational
ICMP based OS fingerprint results: Linux Kernel 2.6.11 (accuracy 100%) Linux Kernel 2.6.10 (accuracy 100%) Linux Kernel 2.6.9 (accuracy 100%) Linux Kernel 2.6.8 (accuracy 100%) Linux Kernel 2.6.7 (accuracy 100%) Linux Kernel 2.6.6 (accuracy 100%) Linux Kernel 2.6.5 (accuracy 100%) Linux Kernel 2.6.4 (accuracy 100%) Linux Kernel 2.6.3 (accuracy 100%) Linux Kernel 2.6.2 (accuracy 100%) Linux Kernel 2.6.1 (accuracy 100%) Linux Kernel 2.6.0 (accuracy 100%) Linux Kernel 2.4.30 (accuracy 100%) Linux Kernel 2.4.29 (accuracy 100%) Linux Kernel 2.4.28 (accuracy 100%) Linux Kernel 2.4.27 (accuracy 100%) Linux Kernel 2.4.26 (accuracy 100%) Linux Kernel 2.4.25 (accuracy 100%) Linux Kernel 2.4.24 (accuracy 100%) Linux Kernel 2.4.23 (accuracy 100%) Linux Kernel 2.4.22 (accuracy 100%) Linux Kernel 2.4.21 (accuracy 100%) Linux Kernel 2.4.20 (accuracy 100%) Linux Kernel 2.4.19 (accuracy 100%) Linux Kernel 2.0.36 (accuracy 100%) Linux Kernel 2.0.34 (accuracy 100%) Linux Kernel 2.0.30 (accuracy 100%) OID : 1.3.6.1.4.1.25623.1.0.102002
Informational
Open TCP ports are 443, 21, 111, 22, 23, 2049, 6000, 25, 80, OID : 1.3.6.1.4.1.25623.1.0.900239
Informational
Nikto could not be found in your system path. OpenVAS was unable to execute Nikto and to perform the scan you requested. Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment.

OID : 1.3.6.1.4.1.25623.1.0.14260

Informational

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
OID : 1.3.6.1.4.1.25623.1.0.80091

[return to alice]

alice - ntp (123/udp)

Informational

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

Risk factor : Low
OID : 1.3.6.1.4.1.25623.1.0.10884

[return to alice]

alice - general/icmp

Informational

Here is the route recorded between 192.168.1.3 and 192.168.1.2 :
192.168.1.2.
192.168.1.2.

OID : 1.3.6.1.4.1.25623.1.0.12264

[return to alice]

Appendix: NVT Information

NVT 1.3.6.1.4.1.25623.1.0.10407: X Server

Summary An X Window System Server is present

Category infos

Family General
Version $Revision: 8046 $
CVE CVE-1999-0526
Signed by • unknown signature

Description

This plugin detects X Window servers.

X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...

An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords.
This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

NVT 1.3.6.1.4.1.25623.1.0.100067: phpMyAdmin DB_Create.PHP Multiple Input Validation Vulnerabilities

Summary Determine if phpMyAdmin is vulnerable to Multiple Input Validation Vulnerabilities
Category infos
Family Web application abuses
Version 1.0
CVE CVE-2007-5976, CVE-2007-5977
BID 26512
Signed by • unknown signature

Description

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities, including a cross-site scripting and a SQL-injection issue.

A successful exploit may allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

These issues affect versions prior to phpMyAdmin 2.11.2.1.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

See also:

http://www.securityfocus.com/bid/26512

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.100068: phpMyAdmin Multiple Input Validation Vulnerabilities

Summary Determine if phpMyAdmin is vulnerable to Multiple Input Validation Vulnerabilities
Category infos
Family Web application abuses
Version 1.0
CVE CVE-2006-6942
BID 21137
Signed by • unknown signature

Description

Overview:
phpMyAdmin is prone to multiple input-validation vulnerabilities,
including an HTML-injection vulnerability, cross-site
scripting vulnerabilities, and information-disclosure
vulnerabilities.

An attacker could exploit these vulnerabilities to view sensitive
information or to have arbitrary script code execute in the context
of the affected site, which may allow the attacker to steal
cookie-based authentication credentials or change the way the site
is rendered to the user. Data gained could aid in further attacks.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:
http://www.securityfocus.com/bid/21137

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.100259: SSH Protocol Versions Supported

Summary Checks for the supported SSH Protocol Versions
Category infos
Family Service detection
Version 1.0
Signed by • unknown signature

Description

Overview:
The remote SSH Server supports the following SSH Protocol Versions:

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.10884: NTP read variables

Summary NTP allows query of variables
Category infos
Family Service detection
Version $Revision: 7516 $
Signed by • unknown signature

Description

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

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.100617: PHP 'php_dechunk()' HTTP Chunked Encoding Integer Overflow Vulnerability

Summary Determine if installed php version is vulnerable
Category infos
Family Web application abuses
Version 1.0-$Revision: 7524 $
BID 39877
Signed by • unknown signature

Description

Overview:
PHP is prone to a remote integer-overflow vulnerability.

An attacker can exploit this issue to execute arbitrary code in the
context of the PHP process. Failed exploit attempts will result in a
denial-of-service condition.

PHP 5.3.0 through 5.3.2 are vulnerable
other versions may also
be affected.

References:
http://www.securityfocus.com/bid/39877
http://php-security.org/2010/05/02/mops-2010-003-php-dechunk-filter-signed-comparison-vulnerability/index.html
http://www.php.net

NVT 1.3.6.1.4.1.25623.1.0.102014: NFS export

Summary Checks for NFS shares
Category infos

Family Remote file access
Version $Revision: 7853 $
CVE CVE-1999-0554, CVE-1999-0548
Signed by • unknown signature

Description

This plugin lists NFS exported shares, and warns if some of
them are readable.

It also warns if the remote NFS server is superfluous.

Tested on Ubuntu/Debian mountd

References:
rfc 1057
rfc 1094

Thanks to Wireshark!

NVT 1.3.6.1.4.1.25623.1.0.100514: Apache Multiple Security Vulnerabilities

Summary Determine if installed Apache version is <= 2.2.14
Category infos
Family Web Servers
Version 1.0-$Revision: 8133 $
CVE CVE-2010-0425, CVE-2010-0434, CVE-2010-0408
BID 38494, 38491
Signed by • unknown signature

Description

Overview:
Apache is prone to multiple vulnerabilities.

These issues may lead to information disclosure or other attacks.

Apache versions prior to 2.2.15-dev are affected.

Solution:
These issues have been addressed in Apache 2.2.15-dev. Apache 2.2.15
including fixes will become available in the future as well. Please
see the references for more information.

References:
http://www.securityfocus.com/bid/38494
http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://svn.apache.org/viewvc?view=revision&revision=917870

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.14371: wu-ftpd MAIL_ADMIN overflow

Summary Checks the banner of the remote wu-ftpd server
Category infos
Family FTP
Version $Revision: 8046 $
CVE CVE-2003-1327
BID 8668
XRefs OSVDB:2594
Signed by • unknown signature

Description

The remote Wu-FTPd server seems to be vulnerable to a remote flaw.

This version fails to properly check bounds on a pathname when Wu-Ftpd is
compiled with MAIL_ADMIN enabled resulting in a buffer overflow. With a
specially crafted request, an attacker can possibly execute arbitrary code
as the user Wu-Ftpd runs as (usually root) resulting in a loss of integrity,
and/or availability.

It should be noted that this vulnerability is not present within the default
installation of Wu-Ftpd.

The server must be configured using the 'MAIL_ADMIN' option to notify an
administrator when a file has been uploaded.

*** OpenVAS solely relied on the banner of the remote server
*** to issue this warning, so it may be a false positive.

Solution : Upgrade to Wu-FTPd 2.6.3 when available
Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.14372: wu-ftpd S/KEY authentication overflow

Summary Checks the banner of the remote wu-ftpd server
Category infos
Family FTP
Version $Revision: 7592 $
CVE CVE-2004-0185
BID 8893
XRefs OSVDB:2715, RHSA:RHSA-2004:096-09, DSA:DSA-457-1
Signed by • unknown signature

Description

The remote Wu-FTPd server seems to be vulnerable to a remote overflow.

This version contains a remote overflow if s/key support is enabled.
The skey_challenge function fails to perform bounds checking on the

name variable resulting in a buffer overflow.
With a specially crafted request, an attacker can execute arbitrary
code resulting in a loss of integrity and/or availability.

It appears that this vulnerability may be exploited prior to authentication.
It is reported that S/Key support is not enabled by default,
though some operating system distributions which ship Wu-Ftpd may have it
enabled.

*** OpenVAS solely relied on the banner of the remote server
*** to issue this warning, so it may be a false positive.

Solution : Upgrade to Wu-FTPd 2.6.3 when available or disable SKEY or apply the
patches available at http://www.wu-ftpd.org

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.12264: Record route

Summary Ping target with Record Route option
Category destructive_attack
Family General
Version $Revision: 7540 $
Signed by • unknown signature

Description

This plugin sends packets with the 'Record Route' option.
It is a complement to traceroute.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.80091: TCP timestamps

Summary Look at RFC1323 TCP timestamps
Category infos
Family General
Version $Revision: 1.5 $
Signed by • unknown signature

Description

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

NVT 1.3.6.1.4.1.25623.1.0.11270: SMTP too long line

Summary Sends a too long single line to the MTA
Category denial
Family SMTP problems
Version $Revision: 7711 $
Signed by • unknown signature

Description

Some antivirus scanners dies when they process an email with a
too long string without line breaks.
Such a message was sent. If there is an antivirus on your MTA,
it might have crashed. Please check its status right now, as
it is not possible to do it remotely

NVT 1.3.6.1.4.1.25623.1.0.800827: Apache 'mod_proxy_http.c' Denial Of Service Vulnerability

Summary Check version of Apache HTTP Server
Category infos
Family Denial of Service
Version $Revision: 1.0 $
CVE CVE-2009-1890
BID 35565
Signed by • unknown signature

Description

Overview:
This host is running Apache HTTP Server and is prone to Denial of Service
vulnerability.

Vulnerability Insight:
The flaw is due to error in 'stream_reqbody_cl' function in 'mod_proxy_http.c'
in the mod_proxy module. When a reverse proxy is configured, it does not properly
handle an amount of streamed data that exceeds the Content-Length value via
crafted requests.

Impact:
Successful exploitation will allow remote attackers to cause Denial of Service
to the legitimate user by CPU consumption.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server version prior to 2.3.3

Fix:
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=790587

References:
http://secunia.com/advisories/35691
http://www.vupen.com/english/advisories/2009/1773
http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.7
Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.100662: PHP Mysqlnd Extension Information Disclosure and Multiple Buffer Overflow Vulnerabilities

Summary Determine if remote php version is vulnerable
Category infos
Family Web application abuses
Version 1.0-$Revision: 7881 $
BID 40461
Signed by • unknown signature

Description

Overview:
The PHP Mysqlnd extension is prone to an information-disclosure
vulnerability and multiple buffer-overflow vulnerabilities.

Successful exploits can allow attackers to obtain sensitive
information or to execute arbitrary code in the context of
applications using the vulnerable PHP functions. Failed attempts may
lead to a denial-of-service condition.

PHP 5.3 through 5.3.2 are vulnerable.

References:
http://www.securityfocus.com/bid/40461
http://php-security.org/2010/05/31/mops-2010-056-php-php_mysqlnd_ok_read-information-leak-vulnerability/index.html
http://php-security.org/2010/05/31/mops-2010-057-php-php_mysqlnd_rset_header_read-buffer-overflow-vulnerability/index.html
http://php-security.org/2010/05/31/mops-2010-058-php-php_mysqlnd_read_error_from_line-buffer-overflow-vulnerability/index.h
http://php-security.org/2010/05/31/mops-2010-059-php-php_mysqlnd_auth_write-stack-buffer-overflow-vulnerability/index.html
http://www.php.net/manual/en/book.mysqlnd.php

http://www.php.net/

NVT 1.3.6.1.4.1.25623.1.0.100643: PHP 'ext/phar/stream.c' and 'ext/phar/dirstream.c' Multiple Format String Vulnerabilities

Summary Determine if installed php version is vulnerable
Category infos
Family Web application abuses
Version 1.0-$Revision: 7721 $
BID 40173
Signed by • unknown signature

Description

Overview:
PHP is prone to multiple format-string vulnerabilities because it fails to properly sanitize user-supplied input before passing it as the format specifier to a formatted-printing function.

Attackers can exploit these issues to run arbitrary code within the context of the PHP process. This may allow them to bypass intended security restrictions or gain elevated privileges.

PHP 5.3 through 5.3.2 are vulnerable.

Solution:
Updates are available
please see the references for details.

References:
http://www.securityfocus.com/bid/40173
http://www.mail-archive.com/php-cvs@lists.php.net/msg46330.html
http://svn.php.net/viewvc?view=revision&revision=298667
http://php-security.org/2010/05/14/mops-2010-024-php-phar_stream_flush-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-025-php-phar_wrapper_open_dir-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-026-php-phar_wrapper_unlink-format-string-vulnerability/index.html
http://php-security.org/2010/05/14/mops-2010-027-php-phar_parse_url-format-string-vulnerabilities/index.html
http://php-security.org/2010/05/14/mops-2010-028-php-phar_wrapper_open_url-format-string-vulnerabilities/index.html
http://www.php.net

NVT 1.3.6.1.4.1.25623.1.0.100074: Check for Telnet Server

Summary Check for Telnet Server
Category infos
Family General
Version 1.0
Signed by • unknown signature

Description

Overview:

A telnet Server is running at this host.

Experts in computer security, such as SANS Institute, and the members of the comp.os.linux.security newsgroup recommend that the use of Telnet for remote logins should be discontinued under all normal circumstances, for the following reasons:

* Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes anybody who
has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login and password information (and whatever else is typed) with any of several common utilities like tcpdump and Wireshark.

* Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.

* Commonly used Telnet daemons have several vulnerabilities discovered over the years.

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.100684: PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability

Summary Determine if php version is <= 5.3.2
Category infos
Family Web application abuses
Version 1.0-$Revision: 8103 $
BID 40948
Signed by • unknown signature

Description

Overview:
PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application. Successful exploits will compromise the application and possibly the computer.

References:
https://www.securityfocus.com/bid/40948
https://bugzilla.redhat.com/show_bug.cgi?id=605641
http://www.php.net

NVT 1.3.6.1.4.1.25623.1.0.900129: phpMyAdmin Detection

Summary Set File Version of phpMyAdmin in KB and report about it
Category infos
Family General

Version Revision: 1.2
Signed by • unknown signature

Description

phpMyAdmin is running at this Host.

phpMyAdmin is a free software tool written in PHP intended to handle
the administration of MySQL over the World Wide Web.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.11111: rpcinfo -p

Summary Dumps all the registered RPC
Category infos
Family RPC
Version $Revision: 7540 $
Signed by • unknown signature

Description

This script calls the DUMP RPC on the port mapper, to obtain the
list of all registered programs.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.10267: SSH Server type and version

Summary SSH Server type and version
Category infos
Family General
Version $Revision: 7589 $
Signed by • unknown signature

Description

This detects the SSH Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the
system they are attacking. Versions and Types should be omitted
where possible.

Solution: Apply filtering to disallow access to this port from untrusted hosts

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.10092: FTP Server type and version

Summary FTP Server type and version
Category infos
Family General
Version $Revision: 7370 $
Signed by • unknown signature

Description

This detects the FTP Server type and version by connecting to the server and
processing the buffer received.
The login banner gives potential attackers additional information about the
system they are attacking. Versions and Types should be omitted
where possible.

Solution: Change the login banner to something generic.

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.100078: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

Summary Determine if phpMyAdmin is vulnerable to Multiple Input Validation
Category infos
Family Web application abuses
Version 1.0
BID 34253
Signed by • unknown signature

Description

Overview:

phpMyAdmin is prone to multiple input-validation vulnerabilities,
including an HTTP response-splitting vulnerability and a
local file-include vulnerability.

These issues can be leveraged to view or execute arbitrary local
scripts, or misrepresent how web content is served, cached, or
interpreted. This could aid in various attacks that try to entice
client users into a false sense of trust. Other attacks are also
possible.

Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Solution:
Vendor updates are available. Please see http://www.phpmyadmin.net for more
Information.

See also:

http://www.securityfocus.com/bid/34253

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.801359: PHP Multiple Information Disclosure Vulnerabilities

Summary Check for the version of PHP
Category infos
Family Web application abuses
Version $Revision: 8025 $
CVE CVE-2010-2190, CVE-2010-2191
Signed by
- unknown signature

Description

Overview: This host is running PHP and is prone to multiple information disclosure vulnerabilities.

Vulnerability Insight:
Multiple flaws are due to:
- Error in 'trim()', 'ltrim()','rtrim()' and 'substr_replace()' functions, which causes a userspace interruption of an internal function within the call time pass by reference feature.
- Error in 'parse_str()', 'preg_match()', 'unpack()' and 'pack()' functions, 'ZEND_FETCH_RW()', 'ZEND_CONCAT()', and 'ZEND_ASSIGN_CONCAT()' opcodes, and the 'ArrayObject::uasort' method, trigger memory corruption by causing a userspace interruption of an internal function or handler.

Impact:
Successful exploitation could allow local attackers to bypass certain security restrictions and to obtain sensitive information.

Impact Level: Network

Affected Software/OS:
PHP version 5.2 through 5.2.13 and 5.3 through 5.3.2

Fix: No solution or patch is available as on 11th June, 2010. Information regarding this issue will be updated once the solution details are available.
For updates refer, http://www.php.net/downloads.php

References:
http://www.php-security.org/2010/05/30/mops-2010-048-php-substr_replace-interruption-information-leak-vulnerability/index.htm
http://www.php-security.org/2010/05/30/mops-2010-047-php-trimltrimrtrim-interruption-information-leak-vulnerability/index.htm

NVT 1.3.6.1.4.1.25623.1.0.10281: Detect Server type and version via Telnet

Summary Detect Server type and version via Telnet
Category infos
Family General
Version $Revision: 7591 $
Signed by
- unknown signature

Description

This detects the Telnet Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the
system they are attacking. Versions and Types should be omitted
where possible.

Solution: Change the login banner to something generic.

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.10263: SMTP Server type and version

Summary SMTP Server type and version
Category infos
Family General
Version $Revision: 7589 $
Signed by
- unknown signature

Description

This detects the SMTP Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the
system they are attacking. Versions and Types should be omitted
where possible.

Solution: Change the login banner to something generic.

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.10330: Services

Summary Find what is listening on which port
Category infos
Family Service detection
Version $Revision: 1852 $
Signed by not signed

Description

This plugin attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 and set the results in the plugins
knowledge base.

Risk factor : None

Parameters

Number of connections done in parallel :	6
Network connection timeout :	5
Network read/write timeout :	5
Wrapped service read timeout :	2

NVT 1.3.6.1.4.1.25623.1.0.102002: OS fingerprinting

Summary Detects remote operating system version
Category infos
Family Service detection
Version 1.0.0
Signed by • unknown signature

Description

This script performs ICMP based OS fingerprinting (as described by
Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine
remote operating system version.

References:
http://www.phrack.org/issues.html?issue=57&id=7#article

NVT 1.3.6.1.4.1.25623.1.0.10415: Sambar sendmail /session/sendmail

Summary Sambar /session/sendmail mailer installed ?
Category attack
Family Web application abuses
Version $Revision: 7540 $
Signed by • unknown signature

Description

The Sambar webserver is running. It provides a web interface for sending emails.
You may simply pass a POST request to /session/sendmail and by this send mails to anyone you want.
Due to the fact that Sambar does not check HTTP referrers you do not need direct access to the server!

Solution : Try to disable this module. There might be a patch in the future.

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.10107: HTTP Server type and version

Summary HTTP Server type and version
Category infos
Family General
Version $Revision: 7515 $
Signed by • unknown signature

Description

This detects the HTTP Server's type and version.

Solution: Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.
With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.900239: Checks for open tcp ports

Summary Check Open TCP Ports
Category infos
Family General
Version $Revision: 8023 $: 1.0
Signed by • unknown signature

Description

Overview: This plugin checks for open tcp ports and reports
the opened ports as well as sets them into the KB.

NVT 1.3.6.1.4.1.25623.1.0.11032: Directory Scanner

Summary Directory Scanner
Category infos
Family Service detection
Version $Revision: 7711 $
XRefs OWASP:OWASP-CM-006
Signed by • unknown signature

Description

This plugin attempts to determine the presence of various
common dirs on the remote web server

NVT 1.3.6.1.4.1.25623.1.0.10662: Web mirroring

Summary Performs a quick web mirror
Category infos
Family Web application abuses
Version $Revision: 7592 $
Signed by • unknown signature

Description

This script makes a mirror of the remote web site(s)
and extracts the list of CGIs that are used by the remote
host.

It is suggested you give a high timeout value to
this plugin and that you change the number of
pages to mirror in the 'Options' section of
the client.

Risk factor : None

Parameters

Number of pages to mirror :	200
Start page :	/

NVT 1.3.6.1.4.1.25623.1.0.11036: SMTP antivirus scanner DoS

Summary	42.zip antivirus MTA DoS
Category	denial
Family	Denial of Service
Version	$Revision: 8045 $
BID	3027
Signed by	• unknown signature

Description

This script sends the 42.zip recursive archive to the
mail server. If there is an antivirus filter, it may start eating huge
amounts of CPU or memory.

Solution: Reconfigure your antivirus / upgrade it

Risk factor : High

NVT 1.3.6.1.4.1.25623.1.0.100631: PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution Vulnerabilities

Summary	Determine if remote php version is vulnerable
Category	infos
Family	Web application abuses
Version	1.0-$Revision: 7609 $
BID	40013
Signed by	• unknown signature

Description

Overview:
PHP is prone to multiple vulnerabilities that may allow

attackers to execute arbitrary code.

Attackers can exploit these issues to run arbitrary code within the
context of the PHP process. This may allow them to bypass intended
security restrictions or gain elevated privileges.

References:
http://www.securityfocus.com/bid/40013
http://php-security.org/2010/05/07/mops-2010-012-php-sqlite_single_query-uninitialized-memory-usage-vulnerability/index.html
http://php-security.org/2010/05/07/mops-2010-013-php-sqlite_array_query-uninitialized-memory-usage-vulnerability/index.html
http://www.php.net
http://php-security.org/2010/05/07/mops-submission-03-sqlite_single_query-sqlite_array_query-uninitialized-memory-usage/index

NVT 1.3.6.1.4.1.25623.1.0.11229: phpinfo.php

Summary Checks for the presence of phpinfo.php
Category infos
Family Web application abuses
Version $Revision: 7518 $
Signed by • unknown signature

Description

Many PHP installation tutorials instruct the user to create
a file called phpinfo.php. This file is often times left in
the root directory after completion.
Some of the information that can be garnered from this file
includes: The username of the user who installed php, if they
are a SUDO user, the IP address of the host, the web server
version, The system version(unix / linux), and the root
directory of the web server.

Solution : remove it
Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.14260: Nikto (NASL wrapper)

Summary Assess web server security with Nikto
Category infos
Family Web application abuses
Version 1.6
Signed by • unknown signature

Description

This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.

Risk factor : None

Parameters

Force scan even without 404s	no

This file was generated by OpenVAS, the free security scanner.