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: Fri Aug 16 12:09:19 2013
Scan finished at: Fri Aug 16 12:34:32 2013

Host	Possible Issues	Holes	Warnings	Notes	False Positives
www.iisgalilei.bz.it	Security hole(s) found	2	14	14	0
Total: 1		2	14	14	0

Reports per Host

www.iisgalilei.bz.it

Scan of this host started at: Fri Aug 16 12:09:23 2013
Scan of this host finished at: Fri Aug 16 12:34:32 2013

Service (Port)	Issue regarding port
ftp (21/tcp)	Security note(s) found
http (80/tcp)	Security hole(s) found
https (443/tcp)	No Information
general/tcp	Security note(s) found
ssh (22/tcp)	No Information
domain (53/udp)	Security note(s) found
general/CPE-T	No Information

[return to summary]

Security Issues and Fixes - Host www.iisgalilei.bz.it

www.iisgalilei.bz.it - ftp (21/tcp)

Informational
An FTP server is running on this port. Here is its banner : 220 FTP Server ready. OID : 1.3.6.1.4.1.25623.1.0.10330
Informational
Remote FTP server banner : 220 FTP Server ready. OID : 1.3.6.1.4.1.25623.1.0.10092

[return to www.iisgalilei.bz.it]

www.iisgalilei.bz.it - http (80/tcp)

Vulnerability

Overview: This host is running phpMyAdmin and is prone to multiple vulnerabilities.

Vulnerability Insight:
Multiple flaws are due to,
- BLOB streaming feature in 'bs_disp_as_mime_type.php' causes CRLF Injection which lets the attacker inject arbitrary data in the HTTP headers through the 'c_type' and 'file_type' parameters.
- XSS Vulnerability in 'display_export.lib.php' as its not sanitizing the 'pma_db_filename_template' parameter.
- Static code injection vulnerability in 'setup.php' which can be used to inject PHP Codes.
- Filename 'bs_disp_as_mime_type.php' which is not sanitizing user supplied inputs in the filename variable which causes directory traversal attacks.

Impact:
Successful exploitation will let the attacker cause XSS, Directory Traversal attacks or can injection malicious PHP Codes to gain sensitive information about the remote host.

Affected Software/OS:
phpMyAdmin version 2.11.x to 2.11.9.4 and 3.0.x to 3.1.3

Fix:
Upgrade to version 2.11.9.5 or 3.1.3.1
http://www.phpmyadmin.net/home_page/downloads.php

Workaround:
Update the existing PHP files from the below SVN Revisions.
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12301
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12302
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12303

*****
Note: Igone the warning, if already replaced according to the fixed svn revision numbers.
*****

References:
http://secunia.com/advisories/34430
http://www.phpmyadmin.net/home_page/security/PMASA-2009-1.php
http://www.phpmyadmin.net/home_page/security/PMASA-2009-2.php
http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 5.5
Risk factor: High
CVE : CVE-2009-1148, CVE-2009-1149, CVE-2009-1150, CVE-2009-1151
BID : 34251, 34253, 34236

OID : 1.3.6.1.4.1.25623.1.0.800381

Vulnerability

Overview: The host is running Apache and is prone to Command Injection vulnerability.

Vulnerability Insight:
The flaw is due to error in the mod_proxy_ftp module which can be exploited via vectors related to the embedding of these commands in the Authorization HTTP header.

Impact:
Successful exploitation could allow remote attackers to bypass intended access restrictions in the context of the affected application, and can cause the arbitrary command injection.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server on Linux.

Fix: Upgrade to Apache HTTP Server version 2.2.15 or later
For updates refer, http://www.apache.org/

References:
http://intevydis.com/vd-list.shtml
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 6.7
Risk factor: High
CVE : CVE-2009-3095
BID : 36254
OID : 1.3.6.1.4.1.25623.1.0.900842

Warning

Overview:
Apache HTTP server is prone to a security-bypass vulnerability related to the handling of specific configuration directives.

A local attacker may exploit this issue to execute arbitrary code within the context of the webserver process. This may result in elevated privileges or aid in further attacks.

Versions prior to Apache 2.2.9 are vulnerable.

Solution:
Updates are available. Please see http://httpd.apache.org/ for more Information.

See also:
http://www.securityfocus.com/bid/35115

Risk factor: Medium
CVE : CVE-2009-1195
BID : 35115
OID : 1.3.6.1.4.1.25623.1.0.100211

Warning

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

Vulnerability Insight :

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

Impact : Remote attackers can execute arbitrary script code.

Impact Level : Application

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

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

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

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

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

Warning

Overview: The host is running Apache and is prone to Denial of Service vulnerability.

Vulnerability Insight:
The flaw is caused due to an error in 'ap_proxy_ftp_handler' function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module while processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.

Impact:
Successful exploitation could allow remote attackers to cause a Denial of
Service in the context of the affected application.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server version 2.0.x to 2.0.63 and and 2.2.x to 2.2.13 on Linux.

Fix: Upgrade to Apache HTTP Server version 2.2.15 or later
For updates refer, http://www.apache.org/

References:
http://intevydis.com/vd-list.shtml
http://www.intevydis.com/blog/?p=59
http://secunia.com/advisories/36549
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score:
CVSS Base Score : 5.4 (AV:N/AC:H/Au:NR/C:N/I:N/A:C)
CVSS Temporal Score : 4.9
Risk factor: Medium
CVE : CVE-2009-3094
BID : 36260
OID : 1.3.6.1.4.1.25623.1.0.900841

Warning

Overview:
phpMyAdmin creates temporary directories and files in an insecure way.

An attacker with local access could potentially exploit this issue to
perform symbolic-link attacks, overwriting arbitrary files in the
context of the affected application.

Successful attacks may corrupt data or cause denial-of-service
conditions. Other unspecified attacks are also possible.

This issue affects phpMyAdmin 2.11.x (prior to 2.11.10.)

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

References:
http://www.securityfocus.com/bid/37826
http://www.phpmyadmin.net/home_page/index.php
http://www.phpmyadmin.net/home_page/security/PMASA-2010-1.php
http://www.phpmyadmin.net/home_page/security/PMASA-2010-2.php

Risk factor : Medium
CVE : CVE-2008-7251, CVE-2008-7252
BID : 37826
OID : 1.3.6.1.4.1.25623.1.0.100450

Warning

Overview:
phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied data.

Exploiting these issues could allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.

Solution:
Vendor updates are available. Please see the references for details.

References:
http://www.securityfocus.com/bid/36658
http://www.phpmyadmin.net/
http://freshmeat.net/projects/phpmyadmin/releases/306669
http://freshmeat.net/projects/phpmyadmin/releases/306667

Risk factor : Low
CVE : CVE-2009-3696
BID : 36658
OID : 1.3.6.1.4.1.25623.1.0.100307

Warning

Overview:
phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability.

An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system; other attacks are also possible.

Versions prior to phpMyAdmin 2.11.9.5 and 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/34236
http://www.securityfocus.com/bid/34251

Risk factor : Medium
CVE : CVE-2009-1151
BID : 34236, 34251
OID : 1.3.6.1.4.1.25623.1.0.100077

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: This host is running phpMyAdmin and is prone to multiple CSRF Injection vulnerability.

Vulnerability Insight:
This flaw is due to failure in sanitizing user-supplied data before being used in the SQL queries via a link or IMG tag to tbl_structure.php with a modified table parameter.

Impact:
Successful exploitation will let the attacker execute arbitrary codes in the context of the application and can compromise database, modify the data or can compromise the whole web application.

Affected Software/OS:
phpMyAdmin, phpMyAdmin version 2.11 to 2.11.9.3 and 3.0 to 3.1.0.9.

Fix:
Upgrade to version 2.11.9.4 or 3.1.1.0
http://www.phpmyadmin.net

References:
http://www.milw0rm.com/exploits/7382
http://www.phpmyadmin.net/home_page/security/PMASA-2008-10.php
https://www.redhat.com/archives/fedora-package-announce/2008-December/msg00784.html

CVSS Score:
CVSS Base Score : 6.0 (AV:N/AC:M/Au:SI/C:P/I:P/A:P)
CVSS Temporal Score : 4.7
Risk factor: Medium
CVE : CVE-2008-5621, CVE-2008-5622
BID : 32720
OID : 1.3.6.1.4.1.25623.1.0.800210

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: This host is running phpMyAdmin and is prone to cross site scripting
vulnerability.

Vulnerability Insight:
Input passed to the 'db' parameter in pmd_pdf.php file is not properly
sanitised before returning to the user.

Impact:

Allows execution of arbitrary HTML and script code, and steal cookie-based
authentication credentials.

Impact Level: System

Affected Software/OS:
phpMyAdmin phpMyAdmin versions 3.0.1 and prior on all running platform.

Fix: Upgrade to phpMyAdmin 3.0.1.1 or later

References:
http://secunia.com/advisories/32449/
http://seclists.org/bugtraq/2008/Oct/0199.html

CVSS Score:
CVSS Base Score : 4.0 (AV:N/AC:H/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 3.2
Risk factor: Medium
CVE : CVE-2008-4775
BID : 31928
OID : 1.3.6.1.4.1.25623.1.0.800301

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 Apache Web Server and is prone to
Information Disclosure Vulnerability.

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

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

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

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

Fix: Upgrade to Apache HTTP Version 2.2.15 or later
For further updates refer, http://httpd.apache.org/download.cgi

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

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

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 'mod_deflate' module which can cause a high CPU
load by requesting large files which are compressed and then disconnecting.

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 2.2.11 and prior

Fix:
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=791454

******
NOTE: Ignore this warning if above mentioned patch is already applied.
******

References:
http://secunia.com/advisories/35781
http://www.vupen.com/english/advisories/2009/1841
https://rhn.redhat.com/errata/RHSA-2009-1148.html
https://bugzilla.redhat.com/show_bug.cgi?id=509125

CVSS Score:
CVSS Base Score : 4.3 (AV:N/AC:M/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.2
Risk factor: Medium
CVE : CVE-2009-1891
BID : 35623
OID : 1.3.6.1.4.1.25623.1.0.800837

Warning

Some Web Servers use a file called /robot(s).txt to make search engines and
any other indexing tools visit their WebPages more frequently and
more efficiently.

By connecting to the server and requesting the /robot(s).txt file, an
attacker may gain additional information about the system they are
attacking.

Such information as, restricted directories, hidden directories, cgi script
directories and etc. Take special care not to tell the robots not to index
sensitive directories, since this tells attackers exactly which of your
directories are sensitive.

The file 'robots.txt' contains the following:
If the Joomla site is installed within a folder such as at
e.g. www.example.com/joomla/ the robots.txt file MUST be
moved to the site root at e.g. www.example.com/robots.txt
AND the joomla folder name MUST be prefixed to the disallowed
path, e.g. the Disallow rule for the /administrator/ folder
MUST be changed to read Disallow: /joomla/administrator/
#
For more information about the robots.txt standard, see:
http://www.robotstxt.org/orig.html
#
For syntax checking, see:
http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/

Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/

Risk factor : Medium
OID : 1.3.6.1.4.1.25623.1.0.10302

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/2.2.3 (CentOS)

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

The following directories were discovered:
/Mail, /News, /ToDo, /adm, /administrator, /asp, /auth, /bak, /cgi, /cgi-bin, /cgis, /db, /demo, /dev, /doc, /includes, /log, /logs, /old, /ssi, /ssl, /stat, /sys, /test, /tmp

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

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. 2.11.3) under /phpmyadmin. (Not protected by Username/Password).

OID : 1.3.6.1.4.1.25623.1.0.900129

Informational

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/iiss/disposizioni-di-legge (searchword [Cerca...] task [search] option [com_search] Itemid [205])
/iiss/esperienze-ed-eventi (searchword [Cerca...] task [search] Itemid [196] format [feed] option [com_search] type [rss])
/iiss/regolamenti-d-istituto (searchword [Cerca...] task [search] option [com_search] Itemid [156])
/iiss/storia-dell-istituto (searchword [Cerca...] task [search] option [com_search] Itemid [157])
/iiss/albo-pretorio (searchword [Cerca...] task [search] option [com_search] Itemid [194])
/iiss/area-genitori (searchword [Cerca...] task [search] option [com_search] Itemid [208])
/iiss/dove-siamo (searchword [Cerca...] task [search] option [com_search] Itemid [161])
/iiss/piano-dell-offerta-formativa (searchword [Cerca...] task [search] option [com_search] Itemid [155])
/iiss/component/search/ (D [A] searchword [Cerca...] task [search] id [10:libri-adottati] Itemid [0] format [opensearch] option [com_search])
/iiss/redazione (searchword [Cerca...] task [search] option [com_search] Itemid [139])
/iiss/contatti-2 (searchword [Cerca...] task [search] option [com_search] Itemid [158])
/iiss/regolamenti (searchword [Cerca...] task [search] option [com_search] Itemid [160])
/iiss/il-dirigente (searchword [Cerca...] task [search] option [com_search] Itemid [138])
/iiss/interni-2 (searchword [Cerca...] task [search] option [com_search] Itemid [159])
/iiss/p-o-f (searchword [Cerca...] task [search] Itemid [209] option [com_search])
/iiss/corsi-di-studio (searchword [Cerca...] task [search] option [com_search] Itemid [114])
/iiss/chi-siamo (searchword [Cerca...] task [search] option [com_search] Itemid [135])
/iiss/indicazioni-per-i-fornitori (searchword [Cerca...] task [search] option [com_search] Itemid [153])
/iiss/corsi-di-studio-2 (searchword [Cerca...] task [search] option [com_search] Itemid [151])
/iiss/viaggi-di-istruzione (searchword [Cerca...] task [search] Itemid [195] format [feed] option [com_search] type [rss])
/iiss/area-studenti (searchword [Cerca...] task [search] option [com_search] Itemid [207])
/iiss/2013-06-01-06-45-16 (searchword [Cerca...] task [search] Itemid [201] format [feed] option [com_search] type [rss])
/iiss/ (searchword [Cerca...] task [search] Itemid [101] format [feed] type [rss] option [com_search])
/iiss/aree-di-progetto (searchword [Cerca...] task [search] Itemid [136] format [feed] option [com_search] type [rss])
/iiss/area-docenti (searchword [Cerca...] task [search] option [com_search] Itemid [206])
/iiss/libri-adottati (searchword [Cerca...] task [search] Itemid [154] option [com_search])
/iiss/piani-di-lavoro-finali-2012-2013 (searchword [Cerca...] task [search] Itemid [218] option [com_search])

OID : 1.3.6.1.4.1.25623.1.0.10662

Informational

Overview:
This host is running Joomla! a widely installed Open Source cms solution.

See also:
http://www.joomla.org

Risk factor : None

Joomla Version (2.5.9.1) with lang(it-IT) was detected on the remote host in the following directory(s):

/

OID : 1.3.6.1.4.1.25623.1.0.100330

Informational

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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

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

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

Solution :

Disable these methods.

See also :

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

Risk factor :

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

Plugin output :

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

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

CVE : CVE-2004-2320, CVE-2003-1567
BID : 9506, 9561, 11604
OID : 1.3.6.1.4.1.25623.1.0.11213

[return to www.iisgalilei.bz.it]

www.iisgalilei.bz.it - general/tcp

Informational
ICMP based OS fingerprint results: HP JetDirect ROM A.03.17 EEPROM A.04.09 (accuracy 70%) HP JetDirect ROM A.05.03 EEPROM A.05.05 (accuracy 70%) HP JetDirect ROM F.08.01 EEPROM F.08.05 (accuracy 70%)

HP JetDirect ROM F.08.08 EEPROM F.08.05 (accuracy 70%)
HP JetDirect ROM F.08.08 EEPROM F.08.20 (accuracy 70%)
HP JetDirect ROM G.05.34 EEPROM G.05.35 (accuracy 70%)
HP JetDirect ROM G.06.00 EEPROM G.06.00 (accuracy 70%)
HP JetDirect ROM G.07.02 EEPROM G.07.17 (accuracy 70%)
HP JetDirect ROM G.07.02 EEPROM G.07.20 (accuracy 70%)
HP JetDirect ROM G.07.02 EEPROM G.08.04 (accuracy 70%)
HP JetDirect ROM G.07.19 EEPROM G.07.20 (accuracy 70%)
HP JetDirect ROM G.07.19 EEPROM G.08.03 (accuracy 70%)
HP JetDirect ROM G.07.19 EEPROM G.08.04 (accuracy 70%)
HP JetDirect ROM G.08.08 EEPROM G.08.04 (accuracy 70%)
HP JetDirect ROM G.08.21 EEPROM G.08.21 (accuracy 70%)
HP JetDirect ROM H.07.15 EEPROM H.08.20 (accuracy 70%)
Linux Kernel 2.6.11 (accuracy 70%)
Linux Kernel 2.6.10 (accuracy 70%)
Linux Kernel 2.6.9 (accuracy 70%)
Linux Kernel 2.6.8 (accuracy 70%)
Linux Kernel 2.6.7 (accuracy 70%)
Linux Kernel 2.6.6 (accuracy 70%)
Linux Kernel 2.6.5 (accuracy 70%)
Linux Kernel 2.6.4 (accuracy 70%)
Linux Kernel 2.6.3 (accuracy 70%)
Linux Kernel 2.6.2 (accuracy 70%)
Linux Kernel 2.6.1 (accuracy 70%)
Linux Kernel 2.6.0 (accuracy 70%)
Linux Kernel 2.4.30 (accuracy 70%)
Linux Kernel 2.4.29 (accuracy 70%)
Linux Kernel 2.4.28 (accuracy 70%)
Linux Kernel 2.4.27 (accuracy 70%)
Linux Kernel 2.4.26 (accuracy 70%)
Linux Kernel 2.4.25 (accuracy 70%)
Linux Kernel 2.4.24 (accuracy 70%)
Linux Kernel 2.4.23 (accuracy 70%)
Linux Kernel 2.4.22 (accuracy 70%)
Linux Kernel 2.4.21 (accuracy 70%)
Linux Kernel 2.4.20 (accuracy 70%)
Linux Kernel 2.4.19 (accuracy 70%)
Linux Kernel 2.0.36 (accuracy 70%)
Linux Kernel 2.0.34 (accuracy 70%)
Linux Kernel 2.0.30 (accuracy 70%)

OID : 1.3.6.1.4.1.25623.1.0.102002

Informational

phpMyAdmin version 2.11.3 running at location /phpmyadmin was detected on the host
OID : 1.3.6.1.4.1.25623.1.0.900129

Informational

Apache Web Server version 2.2.3 was detected on the host
OID : 1.3.6.1.4.1.25623.1.0.900498

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 www.iisgalilei.bz.it]

www.iisgalilei.bz.it - domain (53/udp)

Informational

Overview:
A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.

Risk factor : None
OID : 1.3.6.1.4.1.25623.1.0.100069

[return to www.iisgalilei.bz.it]

Appendix: NVT Information

NVT 1.3.6.1.4.1.25623.1.0.100069: DNS Server Detection

Summary Detect DNS Servers
Category infos
Family General
Version 1.0
Signed by not signed

Description

Overview:
A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of

the website's actual IP address.

Risk factor : None

NVT 1.3.6.1.4.1.25623.1.0.800381: phpMyAdmin Multiple Vulnerabilities

Summary Check for the version of phpMyAdmin
Category infos
Family Web application abuses
Version $Revision: 1.0 $
CVE CVE-2009-1148, CVE-2009-1149, CVE-2009-1150, CVE-2009-1151
BID 34251, 34253, 34236
Signed by not signed

Description

Overview: This host is running phpMyAdmin and is prone to multiple
vulnerabilities.

Vulnerability Insight:
Multiple flaws are due to,
- BLOB streaming feature in 'bs_disp_as_mime_type.php' causes CRLF Injection
which lets the attacker inject arbitrary data in the HTTP headers through
the 'c_type' and 'file_type' parameters.
- XSS Vulnerability in 'display_export.lib.php' as its not sanitizing the
'pma_db_filename_template' parameter.
- Static code injection vulnerability in 'setup.php' which can be used to
inject PHP Codes.
- Filename 'bs_disp_as_mime_type.php' which is not sanitizing user supplied
inputs in the filename variable which causes directory traversal attacks.

Impact:
Successful exploitation will let the attacker cause XSS, Directory Traversal
attacks or can injection malicious PHP Codes to gain sensitive information
about the remote host.

Affected Software/OS:
phpMyAdmin version 2.11.x to 2.11.9.4 and 3.0.x to 3.1.3

Fix:
Upgrade to version 2.11.9.5 or 3.1.3.1
http://www.phpmyadmin.net/home_page/downloads.php

Workaround:
Update the existing PHP files from the below SVN Revisions.
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12301
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12302
http://phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12303

*****
Note: Igone the warning, if already replaced according to the fixed svn
revision numbers.

*****

References:
http://secunia.com/advisories/34430
http://www.phpmyadmin.net/home_page/security/PMASA-2009-1.php
http://www.phpmyadmin.net/home_page/security/PMASA-2009-2.php
http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 5.5
Risk factor: High

NVT 1.3.6.1.4.1.25623.1.0.100330: Joomla! Detection

Summary Checks for the presence of Joomla!
Category infos
Family Service detection
Version 1.0
Signed by not signed

Description

Overview:
This host is running Joomla! a widely installed Open Source cms solution.

See also:
http://www.joomla.org

Risk factor : None

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 not signed

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 1.3.6.1.4.1.25623.1.0.102002: OS fingerprinting

Summary Detects remote operating system version
Category infos
Family Service detection
Version 1.0.0
Signed by not signed

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 1.3.6.1.4.1.25623.1.0.100211: Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability

Summary Check for Apache Web Server version
Category infos
Family Web Servers
Version $Revision: 1.0 $
CVE CVE-2009-1195
BID 35115
Signed by not signed

Description

Overview:
Apache HTTP server is prone to a security-bypass vulnerability
related to the handling of specific configuration directives.

A local attacker may exploit this issue to execute arbitrary code
within the context of the webserver process. This may result in
elevated privileges or aid in further attacks.

Versions prior to Apache 2.2.9 are vulnerable.

Solution:
Updates are available. Please see http://httpd.apache.org/
for more Information.

See also:
http://www.securityfocus.com/bid/35115

Risk factor: Medium

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 not signed

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 1.3.6.1.4.1.25623.1.0.11213: http TRACE XSS attack

Summary http TRACE XSS attack
Category infos
Family Web application abuses
Version $Revision: 8096 $
CVE CVE-2004-2320, CVE-2003-1567
BID 9506, 9561, 11604
Signed by not signed

Description

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

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

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

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

Solution :

Disable these methods.

See also :

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

Risk factor :

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

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 not signed

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 1.3.6.1.4.1.25623.1.0.800210: phpMyAdmin Multiple CSRF SQL Injection Vulnerabilities

Summary Check for the version of phpMyAdmin
Category infos
Family Web application abuses
Version $Revision: 1.0 $
CVE CVE-2008-5621, CVE-2008-5622
BID 32720
Signed by not signed

Description

Overview: This host is running phpMyAdmin and is prone to multiple CSRF Injection vulnerability.

Vulnerability Insight:
This flaw is due to failure in sanitizing user-supplied data before being used in the SQL queries via a link or IMG tag to tbl_structure.php with a modified table parameter.

Impact:
Successful exploitation will let the attacker execute arbitrary codes in the context of the application and can compromise database, modify the data or can compromise the whole web application.

Affected Software/OS:
phpMyAdmin, phpMyAdmin version 2.11 to 2.11.9.3 and 3.0 to 3.1.0.9.

Fix:
Upgrade to version 2.11.9.4 or 3.1.1.0
http://www.phpmyadmin.net

References:
http://www.milw0rm.com/exploits/7382
http://www.phpmyadmin.net/home_page/security/PMASA-2008-10.php
https://www.redhat.com/archives/fedora-package-announce/2008-December/msg00784.html

CVSS Score:
CVSS Base Score : 6.0 (AV:N/AC:M/Au:SI/C:P/I:P/A:P)
CVSS Temporal Score : 4.7
Risk factor: Medium

NVT 1.3.6.1.4.1.25623.1.0.900841: Apache 'mod_proxy_ftp' Module Denial Of Service Vulnerability (Linux)

Summary Check for the version of Apache
Category infos
Family Denial of Service
Version $Revision: 1.0 $
CVE CVE-2009-3094
BID 36260
Signed by not signed

Description

Overview: The host is running Apache and is prone to Denial of Service vulnerability.

Vulnerability Insight:
The flaw is caused due to an error in 'ap_proxy_ftp_handler' function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module while processing responses received from FTP servers. This can be exploited to trigger a NULL-pointer dereference and crash an Apache child process via a malformed EPSV response.

Impact:
Successful exploitation could allow remote attackers to cause a Denial of
Service in the context of the affected application.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server version 2.0.x to 2.0.63 and and 2.2.x to 2.2.13 on Linux.

Fix: Upgrade to Apache HTTP Server version 2.2.15 or later
For updates refer, http://www.apache.org/

References:
http://intevydis.com/vd-list.shtml
http://www.intevydis.com/blog/?p=59
http://secunia.com/advisories/36549
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score:
CVSS Base Score : 5.4 (AV:N/AC:H/Au:NR/C:N/I:N/A:C)
CVSS Temporal Score : 4.9
Risk factor: Medium

NVT 1.3.6.1.4.1.25623.1.0.900107: Apache mod_proxy_ftp Wildcard Characters XSS Vulnerability

Summary Check for vulnerable version of Apache
Category infos
Family Web application abuses
Version $Revision: 1.1 $
CVE CVE-2008-2939
BID 30560
Signed by not signed

Description

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

Vulnerability Insight :

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

Impact : Remote attackers can execute arbitrary script code.

Impact Level : Application

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

***
Note: The script might report a False Positive as it is only checking for

the vulnerable version of Apache. Vulnerability is only when mod_proxy
and mod_proxy_ftp is configured with the installed Apache version.
***

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

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

CVSS Score :
CVSS Base Score : 5.8 (AV:N/AC:M/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 4.5
Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.900842: Apache 'mod_proxy_ftp' Module Command Injection Vulnerability (Linux)

Summary Check for the version of Apache
Category infos
Family General
Version $Revision: 1.0$
CVE CVE-2009-3095
BID 36254
Signed by not signed

Description

Overview: The host is running Apache and is prone to Command Injection
vulnerability.

Vulnerability Insight:
The flaw is due to error in the mod_proxy_ftp module which can be exploited
via vectors related to the embedding of these commands in the Authorization
HTTP header.

Impact:
Successful exploitation could allow remote attackers to bypass intended access
restrictions in the context of the affected application, and can cause the
arbitrary command injection.

Impact Level: Application

Affected Software/OS:
Apache HTTP Server on Linux.

Fix: Upgrade to Apache HTTP Server version 2.2.15 or later
For updates refer, http://www.apache.org/

References:

http://intevydis.com/vd-list.shtml
http://httpd.apache.org/docs/2.0/mod/mod_proxy_ftp.html

CVSS Score:
CVSS Base Score : 7.5 (AV:N/AC:L/Au:NR/C:P/I:P/A:P)
CVSS Temporal Score : 6.7
Risk factor: High

NVT 1.3.6.1.4.1.25623.1.0.100077: phpMyAdmin Code Injection and XSS Vulnerability

Summary Determine if phpMyAdmin is vulnerable to Code Injection
Category infos
Family Web application abuses
Version 1.0
CVE CVE-2009-1151
BID 34236, 34251
Signed by not signed

Description

Overview:
phpMyAdmin is prone to a remote PHP code-injection vulnerability and
to a cross-site scripting vulnerability.

An attacker can exploit this issue to inject and execute arbitrary
malicious PHP code in the context of the webserver process. This may
facilitate a compromise of the application and the underlying
system
other attacks are also possible.

Versions prior to phpMyAdmin 2.11.9.5 and 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/34236
http://www.securityfocus.com/bid/34251

Risk factor : Medium

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 1.3.6.1.4.1.25623.1.0.800301: phpMyAdmin pmd_pdf.php Cross Site Scripting Vulnerability

Summary	Check for the Version of phpMyAdmin
Category	infos
Family	Web application abuses
Version	$Revision: 1.0 $
CVE	CVE-2008-4775
BID	31928
Signed by	not signed

Description

Overview: This host is running phpMyAdmin and is prone to cross site scripting
vulnerability.

Vulnerability Insight:
Input passed to the 'db' parameter in pmd_pdf.php file is not properly
sanitised before returning to the user.

Impact:
Allows execution of arbitrary HTML and script code, and steal cookie-based
authentication credentials.

Impact Level: System

Affected Software/OS:
phpMyAdmin phpMyAdmin versions 3.0.1 and prior on all running platform.

Fix: Upgrade to phpMyAdmin 3.0.1.1 or later

References:
http://secunia.com/advisories/32449/
http://seclists.org/bugtraq/2008/Oct/0199.html

CVSS Score:
CVSS Base Score : 4.0 (AV:N/AC:H/Au:NR/C:P/I:P/A:N)
CVSS Temporal Score : 3.2
Risk factor: Medium

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 not signed

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 1.3.6.1.4.1.25623.1.0.100307: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities

Summary Determine if phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities
Category infos
Family Web application abuses
Version 1.0-$Revision: 8287 $
CVE CVE-2009-3696
BID 36658
Signed by not signed

Description

Overview:
phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user-supplied data.

Exploiting these issues could allow an attacker to steal cookie-based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.

Solution:
Vendor updates are available. Please see the references for details.

References:
http://www.securityfocus.com/bid/36658
http://www.phpmyadmin.net/
http://freshmeat.net/projects/phpmyadmin/releases/306669
http://freshmeat.net/projects/phpmyadmin/releases/306667

Risk factor : Low

NVT 1.3.6.1.4.1.25623.1.0.100450: phpMyAdmin Insecure Temporary File and Directory Creation Vulnerabilities

Summary Determine if phpMyAdmin version is < 2.11.10
Category infos
Family Web application abuses
Version 1.0-$Revision: 8287 $
CVE CVE-2008-7251, CVE-2008-7252
BID 37826
Signed by not signed

Description

Overview:
phpMyAdmin creates temporary directories and files in an insecure way.

An attacker with local access could potentially exploit this issue to
perform symbolic-link attacks, overwriting arbitrary files in the
context of the affected application.

Successful attacks may corrupt data or cause denial-of-service
conditions. Other unspecified attacks are also possible.

This issue affects phpMyAdmin 2.11.x (prior to 2.11.10.)

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

References:
http://www.securityfocus.com/bid/37826
http://www.phpmyadmin.net/home_page/index.php
http://www.phpmyadmin.net/home_page/security/PMASA-2010-1.php
http://www.phpmyadmin.net/home_page/security/PMASA-2010-2.php

Risk factor : Medium

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 not signed

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 1.3.6.1.4.1.25623.1.0.100078: 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 not signed

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 1.3.6.1.4.1.25623.1.0.800827: 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 not signed

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 1.3.6.1.4.1.25623.1.0.900499: Apache mod_proxy_ajp Information Disclosure Vulnerability

Summary Check for Apache Web Server version
Category infos
Family Web application abuses
Version $Revision: 1.0 $
CVE CVE-2009-1191
BID 34663
Signed by not signed

Description

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

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

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

Impact level: Application

Affected Software/OS:
Apache HTTP Version 2.2.11

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

Fix: Upgrade to Apache HTTP Version 2.2.15 or later
For further updates refer, http://httpd.apache.org/download.cgi

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

CVSS Score:
CVSS Base Score : 5.0 (AV:N/AC:L/Au:NR/C:P/I:N/A:N)
CVSS Temporal Score : 4.0
Risk factor: Medium

NVT 1.3.6.1.4.1.25623.1.0.800837: Apache 'mod_deflate' Denial Of Service Vulnerability - July09

Summary Check version of Apache HTTP Server
Category infos
Family Denial of Service
Version $Revision: 1.0 $
CVE CVE-2009-1891
BID 35623
Signed by not signed

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 'mod_deflate' module which can cause a high CPU load by requesting large files which are compressed and then disconnecting.

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 2.2.11 and prior

Fix:
Fixed in the SVN repository.
http://svn.apache.org/viewvc?view=rev&revision=791454

******
NOTE: Ignore this warning if above mentioned patch is already applied.
******

References:
http://secunia.com/advisories/35781
http://www.vupen.com/english/advisories/2009/1841
https://rhn.redhat.com/errata/RHSA-2009-1148.html
https://bugzilla.redhat.com/show_bug.cgi?id=509125

CVSS Score:
CVSS Base Score : 4.3 (AV:N/AC:M/Au:NR/C:N/I:N/A:P)
CVSS Temporal Score : 3.2
Risk factor: Medium

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 not signed

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 1.3.6.1.4.1.25623.1.0.10302: robot(s).txt exists on the Web Server

Summary robot(s).txt exists on the Web Server
Category attack
Family General
Version $Revision: 7592 $
Signed by not signed

Description

Some Web Servers use a file called /robot(s).txt to make search engines and
any other indexing tools visit their WebPages more frequently and
more efficiently.

By connecting to the server and requesting the /robot(s).txt file, an
attacker may gain additional information about the system they are
attacking.

Such information as, restricted directories, hidden directories, cgi script
directories and etc. Take special care not to tell the robots not to index
sensitive directories, since this tells attackers exactly which of your
directories are sensitive.

Risk factor : Medium

NVT 1.3.6.1.4.1.25623.1.0.900498: Apache Web ServerVersion Detection

Summary Set Version of Apache Web Server in KB
Category infos
Family Service detection
Version Revision: 1.0
Signed by not signed

Description

Overview : This script finds the running Apache Version and saves the result in KB.

Risk factor : None

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 not signed

Description

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

---

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