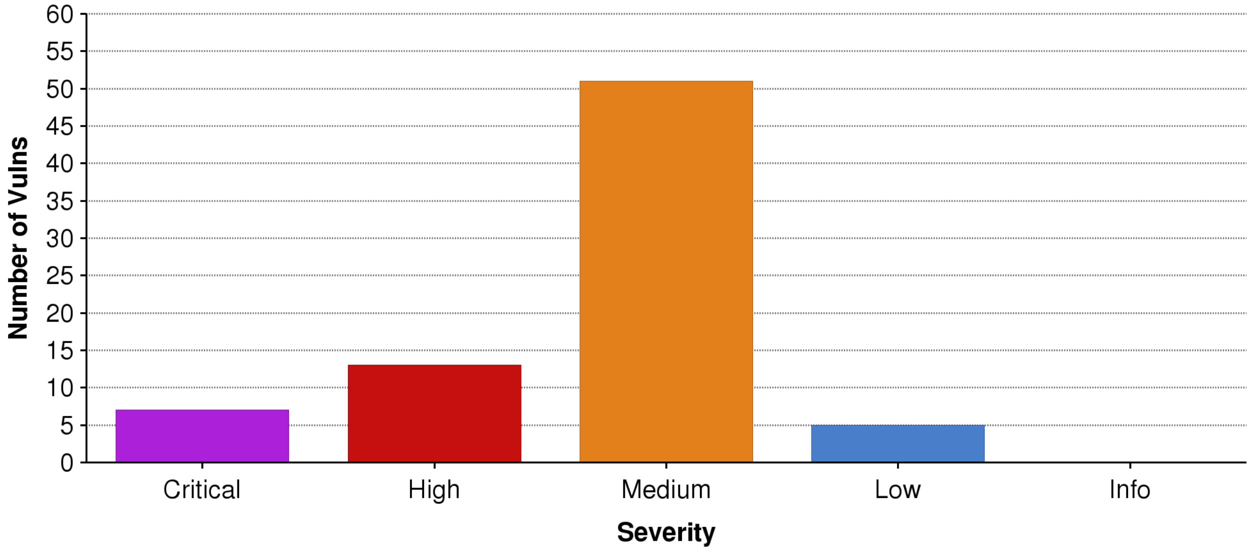
CIT

Telmax vulnerability Report

November 14, 2013 at 6:22pm EST
Org Head CIT [ohcit]

Summary

Pie Chart



Vulnerability Summary

Vulnerability Summary - Critical

Severity	Plugin Name	Family
Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
Critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers
Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
Critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers
Critical	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.

Vulnerability Summary - High

Severity	Plugin Name	Family
High	PHP < 5.2.6 Multiple Vulnerabilities	CGI abuses
High	PHP 5 < 5.2.7 Multiple Vulnerabilities	CGI abuses
High	PHP < 5.2.8 Multiple Vulnerabilities	CGI abuses
High	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses
High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
High	Apache 2.2 < 2.2.14 Multiple Vulnerabilities	Web Servers
High	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses
High	Apache HTTP Server Byte Range DoS	Web Servers
High	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses

Vulnerability Summary - Medium

Severity	Plugin Name	Family
Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
Medium	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Web Servers
Medium	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Web Servers
Medium	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Web Servers
Medium	Apache < 2.2.8 Multiple Vulnerabilities (XSS, DoS)	Web Servers
Medium	Apache < 2.2.8 Multiple Vulnerabilities (XSS, DoS)	Web Servers
Medium	Apache < 2.2.8 Multiple Vulnerabilities (XSS, DoS)	Web Servers
Medium	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	Web Servers
Medium	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	Web Servers
Medium	Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)	Web Servers
Medium	PHP < 5.2.9 Multiple Vulnerabilities	CGI abuses
Medium	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses
Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.x < 2.2.12 Multiple Vulnerabilities	Web Servers
Medium	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS	Misc.
Medium	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses
Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CGI abuses
Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.16 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers

Severity	Plugin Name	Family
Medium	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CGI abuses
Medium	SSL Certificate Cannot Be Trusted	General
Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CGI abuses
Medium	OpenSSL SSL_OP_NETSCAPE_REUSE_ Ciphersuite Disabled Cipher Issue	General
Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers
Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers
Medium	Apache 2.2 < 2.2.18 APR apr_fnmatch DoS	Web Servers
Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Web Servers
Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Web Servers
Medium	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Web Servers
Medium	SMB Signing Disabled	Misc.
Medium	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	Web Servers
Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
Medium	Apache 2.2 < 2.2.23 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.23 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.23 Multiple Vulnerabilities	Web Servers
Medium	TLS CRIME Vulnerability	General
Medium	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities	Web Servers

Severity	Plugin Name	Family
Medium	Apache 2.2 < 2.2.25 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.25 Multiple Vulnerabilities	Web Servers
Medium	Apache 2.2 < 2.2.25 Multiple Vulnerabilities	Web Servers

Vulnerability Details

Details - Critical Vulnerabilities

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Critical	10.3.0.122	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.15
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6750, CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434

BID: 21865, 36935, 38491, 38494, 38580

Crossref: OSVDB #59969, OSVDB #62674, OSVDB #62675, OSVDB #62676, Secunia #38776, CWE #200

Vulnerability Publication Date: 2010/03/03

Patch Publication Date: 2010/03/08

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/09/24

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_15.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3555,CVE-2010-0408,CVE-2010-0434,CVE-2010-0425,CVE-2007-6750

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 3, 2010 12:00:00 EST

Patch Publication Date: Mar 8, 2010 12:00:00 EST

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Sep 24, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache mod_isapi <= 2.2.14 Dangling Pointer), Core Impact

Check Type: remote

Version: Revision: 1.24

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Critical	10.3.0.122	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.15
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6750, CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434

BID: 21865, 36935, 38491, 38494, 38580

Crossref: OSVDB #59969, OSVDB #62674, OSVDB #62675, OSVDB #62676, Secunia #38776, CWE #200

Vulnerability Publication Date: 2010/03/03

Patch Publication Date: 2010/03/08

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/09/24

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_15.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3555,CVE-2010-0408,CVE-2010-0434,CVE-2010-0425,CVE-2007-6750

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 3, 2010 12:00:00 EST

Patch Publication Date: Mar 8, 2010 12:00:00 EST

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Sep 24, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache mod_isapi <= 2.2.14 Dangling Pointer), Core Impact

Check Type: remote

Version: Revision: 1.24

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.15	Critical	10.3.0.122	8457	TCP	Web Servers	Yes

Multiple
Vulnerabilities

MAC Address: 00:50:56:8b:1c:9d

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 8.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.15
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6750, CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434

BID: 21865, 36935, 38491, 38494, 38580

Crossref: OSVDB #59969, OSVDB #62674, OSVDB #62675, OSVDB #62676, Secunia #38776, CWE #200

Vulnerability Publication Date: 2010/03/03

Patch Publication Date: 2010/03/08

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/09/24

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_15.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities :

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.15 or later.

See Also: http://httpd.apache.org/security/vulnerabilities_22.html
https://issues.apache.org/bugzilla/show_bug.cgi?id=48359
http://www.nessus.org/u?0bf1f184

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3555,CVE-2010-0408,CVE-2010-0434,CVE-2010-0425,CVE-2007-6750

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 3, 2010 12:00:00 EST

Patch Publication Date: Mar 8, 2010 12:00:00 EST

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Sep 24, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache mod_isapi <= 2.2.14 Dangling Pointer), Core Impact

Check Type: remote

Version: Revision: 1.24

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Critical	10.3.0.122	80	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.4

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.13

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

BID: 35949

Crossref: OSVDB #56765, CWE #189

Vulnerability Publication Date: 2009/08/04

Patch Publication Date: 2009/08/09

Plugin Publication Date: 2012/01/19

Plugin Modification Date: 2012/01/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_13.nasl

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Aug 4, 2009 12:00:00 EDT

Patch Publication Date: Aug 9, 2009 12:00:00 EDT

Plugin Publication Date: Jan 19, 2012 12:00:00 EST

Plugin Modification Date: Jan 20, 2012 12:00:00 EST

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.2

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Critical	10.3.0.122	443	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.4

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.13
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

BID: 35949

Crossref: OSVDB #56765, CWE #189

Vulnerability Publication Date: 2009/08/04

Patch Publication Date: 2009/08/09

Plugin Publication Date: 2012/01/19

Plugin Modification Date: 2012/01/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_13.nasl

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Aug 4, 2009 12:00:00 EDT

Patch Publication Date: Aug 9, 2009 12:00:00 EDT

Plugin Publication Date: Jan 19, 2012 12:00:00 EST

Plugin Modification Date: Jan 20, 2012 12:00:00 EST

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.2

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.13 APR apr_palloc	Critical	10.3.0.122	8457	TCP	Web Servers	No

Heap
Overflow

MAC Address: 00:50:56:8b:1c:9d

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.4

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.13
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

BID: 35949

Crossref: OSVDB #56765, CWE #189

Vulnerability Publication Date: 2009/08/04

Patch Publication Date: 2009/08/09

Plugin Publication Date: 2012/01/19

Plugin Modification Date: 2012/01/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_13.nasl

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

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

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

Solution: Upgrade to Apache 2.2.13 or later.

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

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2412

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Aug 4, 2009 12:00:00 EDT

Patch Publication Date: Aug 9, 2009 12:00:00 EDT

Plugin Publication Date: Jan 19, 2012 12:00:00 EST

Plugin Modification Date: Jan 20, 2012 12:00:00 EST

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.2

Plugin Name	Severity	IP Address	Port	Protocol	Family	Exploit?
Samba 'AndX' Request Heap-Based Buffer Overflow	Critical	10.3.0.122	445	TCP	Misc.	No

MAC Address: 00:50:56:8b:1c:9d

Synopsis: The remote Samba service is vulnerable to a heap overflow attack.

Description: The remote Samba install is prone to a heap-based buffer overflow attack.

An attacker can exploit this issue to execute arbitrary code with the privileges of the application. Failed exploit attempts will result in a denial of service condition.

Solution: Apply patches from the vendor.

See Also: https://www.samba.org/samba/security/CVE-2012-0870.html
https://www.samba.org/samba/history/security.html

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 7.4

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

CPE: cpe:/a:samba:samba

CVE: CVE-2012-0870

BID: 52103

Crossref: OSVDB #79443

Vulnerability Publication Date: 2012/02/21

Patch Publication Date: 2012/02/21

Plugin Publication Date: 2012/03/13

Plugin Modification Date: 2012/11/12

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: samba_andx_heap_overflow.nbin

Synopsis: The remote Samba service is vulnerable to a heap overflow attack.

Description: The remote Samba install is prone to a heap-based buffer overflow attack.

An attacker can exploit this issue to execute arbitrary code with the privileges of the application. Failed exploit attempts will result in a denial of service condition.

Solution: Apply patches from the vendor.

See Also: https://www.samba.org/samba/security/CVE-2012-0870.html
https://www.samba.org/samba/history/security.html

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C

CPE: cpe:/a:samba:samba

CVE: CVE-2012-0870

First Discovered: Apr 2, 2012 13:27:46 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Feb 21, 2012 12:00:00 EST

Patch Publication Date: Feb 21, 2012 12:00:00 EST

Plugin Publication Date: Mar 13, 2012 12:00:00 EDT

Plugin Modification Date: Nov 12, 2012 12:00:00 EST

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.4

Details - High Vulnerabilities

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.2.6 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

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

- A stack buffer overflow in FastCGI SAPI.

- An integer overflow in printf().

- An security issue arising from improper calculation
of the length of PATH_TRANSLATED in cgi_main.c.

- A safe_mode bypass in cURL.

- Incomplete handling of multibyte chars inside
escapeshellcmd().

- Issues in the bundled PCRE fixed by version 7.6.

See also :

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

Solution :

Upgrade to PHP version 5.2.6 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.6
```

CVE : CVE-2007-4850, CVE-2007-6039, CVE-2008-0599, CVE-2008-1384, CVE-2008-2050, CVE-2008-2051
BID : 27413, 28392, 29009

Other references : OSVDB:43219, OSVDB:44057, OSVDB:44906, OSVDB:44907, OSVDB:44908, OSVDB:45304, OSVDB:45305, Secunia:30048, CWE:264

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

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

- A stack buffer overflow in FastCGI SAPI.

- An integer overflow in printf().

- An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c.

- A safe_mode bypass in cURL.

- Incomplete handling of multibyte chars inside escapeshellcmd().

- Issues in the bundled PCRE fixed by version 7.6.

Solution: Upgrade to PHP version 5.2.6 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2008-2051,CVE-2008-1384,CVE-2008-2050,CVE-2007-4850,CVE-2008-0599,CVE-2007-6039

BID: 29009,27413,28392

Cross References: OSVDB #44906,OSVDB #44907,OSVDB #44908,OSVDB #43219,CWE #264,OSVDB #44057,OSVDB #45304,OSVDB #45305,Secunia #30048

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: May 2, 2008 12:00:00 EDT

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.22

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP 5 < 5.2.7 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote
host is older than 5.2.7. Such versions may be affected by several
security issues :

- File truncation can occur when calling 'dba_replace()'
with an invalid argument.

- There is a buffer overflow in the bundled PCRE library
fixed by 7.8. (CVE-2008-2371)

- A buffer overflow in the 'imageloadfont()' function in
'ext/gd/gd.c' can be triggered when a specially crafted
font is given. (CVE-2008-3658)

- There is a buffer overflow in PHP's internal function
'memnstr()', which is exposed to userspace as
'explode()'. (CVE-2008-3659)

- When used as a FastCGI module, PHP segfaults when
opening a file whose name contains two dots (eg,
'file..php'). (CVE-2008-3660)

- Multiple directory traversal vulnerabilities in
functions such as 'posix_access()', 'chdir()', 'ftok()'
may allow a remote attacker to bypass 'safe_mode'
restrictions. (CVE-2008-2665 and CVE-2008-2666).

- A buffer overflow may be triggered when processing long
message headers in 'php_imap.c' due to use of an
obsolete API call. (CVE-2008-2829)

- A heap-based buffer overflow may be triggered via
a call to 'mb_check_encoding()', part of the 'mbstring'
extension. (CVE-2008-5557)

- Missing initialization of 'BG(page_uid)' and
'BG(page_gid)' when PHP is used as an Apache module
may allow for bypassing security restriction due to
SAPI 'php_getuid()' overloading. (CVE-2008-5624)

- Incorrect 'php_value' order for Apache configuration
may allow bypassing PHP's 'safe_mode' setting.
(CVE-2008-5625)

- The ZipArchive:extractTo() method in the ZipArchive
extension fails to filter directory traversal
sequences from file names. (CVE-2008-5658)

See also :

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

http://bugs.php.net/bug.php?id=45151
http://bugs.php.net/bug.php?id=45722
http://www.php.net/releases/5_2_7.php
http://www.php.net/ChangeLog-5.php#5.2.7

Solution :

Upgrade to PHP version 5.2.8 or later.

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

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.7

CVE : CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658
BID : 29796, 29797, 29829, 30087, 30649, 31612, 32383, 32625, 32688, 32948
Other references : OSVDB:46584, OSVDB:46638, OSVDB:46639, OSVDB:46641, OSVDB:46690, OSVDB:47796, OSVDB:47797, OSVDB:47798, OSVDB:50480, OSVDB:51477, OSVDB:52205, OSVDB:52206, OSVDB:52207, CWE:119

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

Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.7. Such versions may be affected by several security issues :

- File truncation can occur when calling 'dba_replace()' with an invalid argument.

- There is a buffer overflow in the bundled PCRE library fixed by 7.8. (CVE-2008-2371)

- A buffer overflow in the 'imageloadfont()' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. (CVE-2008-3658)

- There is a buffer overflow in PHP's internal function 'memnstr()', which is exposed to userspace as 'explode()'. (CVE-2008-3659)

- When used as a FastCGI module, PHP segfaults when opening a file whose name contains two dots (eg, 'file..php'). (CVE-2008-3660)

- Multiple directory traversal vulnerabilities in functions such as 'posix_access()', 'chdir()', 'ftok()' may allow a remote attacker to bypass 'safe_mode' restrictions. (CVE-2008-2665 and CVE-2008-2666).

- A buffer overflow may be triggered when processing long message headers in 'php_imap.c' due to use of an obsolete API call. (CVE-2008-2829)

- A heap-based buffer overflow may be triggered via a call to 'mb_check_encoding()', part of the 'mbstring' extension. (CVE-2008-5557)

- Missing initialization of 'BG(page_uid)' and 'BG(page_gid)' when PHP is used as an Apache module may allow for bypassing security restriction due to SAPI 'php_getuid()' overloading. (CVE-2008-5624)

- Incorrect 'php_value' order for Apache configuration may allow bypassing PHP's 'safe_mode' setting.
(CVE-2008-5625)

- The ZipArchive:extractTo() method in the ZipArchive extension fails to filter directory traversal sequences from file names. (CVE-2008-5658)

Solution: Upgrade to PHP version 5.2.8 or later.

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

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE:
CVE-2008-3658,CVE-2008-3660,CVE-2008-5557,CVE-2008-2371,CVE-2008-2665,CVE-2008-2666,CVE-2008-2829,CVE-2008-3

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

Cross References: OSVDB #46584,OSVDB #46638,OSVDB #46639,OSVDB #50480,OSVDB #51477,OSVDB #46641,OSVDB #46690,OSVDB #47796,OSVDB #47797,OSVDB #47798,CWE #119,OSVDB #52205,OSVDB #52207,OSVDB #52206

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Dec 5, 2008 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.22

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.2.8 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote
host is earlier than 5.2.8. As such, it is potentially affected by
the following vulnerabilities :

- PHP fails to properly sanitize error messages of
arbitrary HTML or script code, would code allow for
cross-site scripting attacks if PHP's 'display_errors'
setting is enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to
'magic_quotes' functionality due to an incorrect fix to
the filter extension. As a result, the
'magic_quotes_gpc' setting remains off even if it is set
to on. (CVE-2008-5844)

See also :

http://bugs.php.net/42718
http://www.php.net/releases/5_2_8.php

Solution :

Upgrade to PHP version 5.2.8 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.8

CVE : CVE-2008-5814, CVE-2008-5844
BID : 32673
Other references : OSVDB:50587, OSVDB:53532, CWE:16

Synopsis: The remote web server uses a version of PHP that may be affected by multiple vulnerabilities.

Description: According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :

- PHP fails to properly sanitize error messages of arbitrary HTML or script code, would code allow for cross-site scripting attacks if PHP's 'display_errors' setting is enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to 'magic_quotes' functionality due to an incorrect fix to the filter extension. As a result, the 'magic_quotes_gpc' setting remains off even if it is set to on. (CVE-2008-5844)

Solution: Upgrade to PHP version 5.2.8 or later.

See Also: http://bugs.php.net/42718
http://www.php.net/releases/5_2_8.php

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C
CPE: cpe:/a:php:php
CVE: CVE-2008-5844,CVE-2008-5814
BID: 32673
Cross References: CWE #16,OSVDB #53532,OSVDB #50587
First Discovered: Feb 6, 2012 10:20:49 EST
Last Observed: Jul 2, 2012 13:28:13 EDT
Vuln Publication Date: N/A
Patch Publication Date: N/A
Plugin Publication Date: Dec 9, 2008 12:00:00 EST
Plugin Modification Date: Oct 23, 2013 12:00:00 EDT
Exploit Ease: Exploits are available
Exploit Frameworks:
Check Type: remote
Version: Revision: 1.15

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.2.11 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	No

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.

- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.

- An unspecified input validation vulnerability affects exif processing.

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

- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)

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

See also :

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

http://www.php.net/ChangeLog-5.php#5.2.11

Solution :

Upgrade to PHP version 5.2.11 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.5
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.11

CVE : CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, CVE-2009-5016
BID : 36449, 44889
Other references : OSVDB:58185, OSVDB:58186, OSVDB:58187, OSVDB:58188, OSVDB:60438, OSVDB:69227, Secunia:36791, CWE:20

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

Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.

- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.

- An unspecified input validation vulnerability affects exif processing.

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

- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)

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

Solution: Upgrade to PHP version 5.2.11 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 5.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:U/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2009-4018,CVE-2009-3291,CVE-2009-3292,CVE-2009-3293,CVE-2009-3294,CVE-2009-5016

BID: 36449,44889

Cross References: OSVDB #58185,OSVDB #58187,OSVDB #60438,CWE #20,OSVDB #58188,OSVDB #58186,OSVDB #69227,Secunia #36791

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT
Vuln Publication Date: N/A
Patch Publication Date: Sep 16, 2009 12:00:00 EDT
Plugin Publication Date: Sep 18, 2009 12:00:00 EDT
Plugin Modification Date: Oct 23, 2013 12:00:00 EDT
Exploit Ease: No known exploits are available
Exploit Frameworks:
Check Type: remote
Version: Revision: 1.16

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
Apache 2.2 < 2.2.14 Multiple Vulnerabilities	High	10.3.0.122	80	TCP	Yes

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

CVSS Base Score: 7.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 6.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.14

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2699, CVE-2009-3094, CVE-2009-3095

BID: 36254, 36260, 36596

Crossref: OSVDB #57851, OSVDB #57882, OSVDB #58879, Secunia #36549, CWE #264

Vulnerability Publication Date: 2009/10/05

Patch Publication Date: 2009/10/05

Plugin Publication Date: 2009/10/07

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_14.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3094,CVE-2009-3095,CVE-2009-2699

BID: 36254,36260,36596

Cross References: OSVDB #57851,OSVDB #58879,CWE #264,OSVDB #57882,Secunia #36549

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2009 12:00:00 EDT

Patch Publication Date: Oct 5, 2009 12:00:00 EDT

Plugin Publication Date: Oct 7, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.23

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
Apache 2.2 < 2.2.14 Multiple Vulnerabilities	High	10.3.0.122	443	TCP	Yes

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

CVSS Base Score: 7.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 6.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.14
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2699, CVE-2009-3094, CVE-2009-3095

BID: 36254, 36260, 36596

Crossref: OSVDB #57851, OSVDB #57882, OSVDB #58879, Secunia #36549, CWE #264

Vulnerability Publication Date: 2009/10/05

Patch Publication Date: 2009/10/05

Plugin Publication Date: 2009/10/07

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_14.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3094,CVE-2009-3095,CVE-2009-2699

BID: 36254,36260,36596

Cross References: OSVDB #57851,OSVDB #58879,CWE #264,OSVDB #57882,Secunia #36549

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2009 12:00:00 EDT

Patch Publication Date: Oct 5, 2009 12:00:00 EDT

Plugin Publication Date: Oct 7, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.23

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
Apache 2.2 < 2.2.14 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

CVSS Base Score: 7.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 6.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.14
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-2699, CVE-2009-3094, CVE-2009-3095

BID: 36254, 36260, 36596

Crossref: OSVDB #57851, OSVDB #57882, OSVDB #58879, Secunia #36549, CWE #264

Vulnerability Publication Date: 2009/10/05

Patch Publication Date: 2009/10/05

Plugin Publication Date: 2009/10/07

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_14.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.14. Such versions are potentially affected by multiple vulnerabilities :

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)

- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)

- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

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

Solution: Either ensure the affected modules are not in use or upgrade to Apache version 2.2.14 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3094,CVE-2009-3095,CVE-2009-2699

BID: 36254,36260,36596

Cross References: OSVDB #57851,OSVDB #58879,CWE #264,OSVDB #57882,Secunia #36549

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2009 12:00:00 EDT

Patch Publication Date: Oct 5, 2009 12:00:00 EDT

Plugin Publication Date: Oct 7, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.23

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP 5.2 < 5.2.14 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

According to its banner, the version of PHP 5.2 installed on the
remote host is older than 5.2.14. Such versions may be affected by
several security issues :

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

- An error exists in the function 'fnmatch' that can lead to stack exhaustion.

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

- A memory corruption error exists in the function 'substr_replace'.

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

addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, strstr, str_pad, str_word_count, wordwrap, strtok, setcookie, strip_tags, trim, ltrim, rtrim, parse_str, pack, unpack, uasort, preg_match, strrchr, strchr, substr, str_repeat (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)

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

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

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

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

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

See also :

http://www.php.net/releases/5_2_14.php
http://www.php.net/ChangeLog-5.php#5.2.14

Solution :

Upgrade to PHP version 5.2.14 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.14
```

CVE : CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065
BID : 38708, 40948, 41991
Other references : OSVDB:33942, OSVDB:63078, OSVDB:64322, OSVDB:64544, OSVDB:64546, OSVDB:65755, OSVDB:66087, OSVDB:66093, OSVDB:66094, OSVDB:66095, OSVDB:66096, OSVDB:66097, OSVDB:66098, OSVDB:66099, OSVDB:66100, OSVDB:66101, OSVDB:66102, OSVDB:66103, OSVDB:66104, OSVDB:66105, OSVDB:66106, OSVDB:66798, OSVDB:66804, OSVDB:66805, Secunia:39675, Secunia:40268

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

Description: According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.14. Such versions may be affected by several security issues :

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

- An error exists in the function 'fnmatch' that can lead to stack exhaustion.

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

- A memory corruption error exists in the function 'substr_replace'.

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

addcslashes, chunk_split, html_entity_decode, iconv_mime_decode, iconv_substr, iconv_mime_encode, htmlentities, htmlspecialchars, str_getcsv, http_build_query, strpbrk, strstr, str_pad, str_word_count, wordwrap, strtok, setcookie, strip_tags, trim, ltrim, rtrim, parse_str, pack, unpack, uasort, preg_match, strrchr, strchr, substr, str_repeat (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)

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

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

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

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

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

Solution: Upgrade to PHP version 5.2.14 or later.

See Also: http://www.php.net/releases/5_2_14.php
http://www.php.net/ChangeLog-5.php#5.2.14

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE:
CVE-2010-0397,CVE-2010-2225,CVE-2010-2531,CVE-2010-1860,CVE-2010-1862,CVE-2010-1864,CVE-2010-2097,CVE-2010-2

BID: 38708,40948,41991

Cross References: OSVDB #66798,OSVDB #66804,OSVDB #66805,OSVDB #63078,OSVDB #65755,OSVDB #33942,OSVDB #64322,OSVDB #64544,OSVDB #64546,OSVDB #66087,OSVDB #66093,OSVDB #66094,OSVDB #66095,OSVDB #66096,OSVDB #66097,OSVDB #66098,OSVDB #66099,OSVDB #66100,OSVDB #66101,OSVDB #66102,OSVDB #66103,OSVDB #66104,OSVDB #66105,OSVDB #66106,Secunia #39675,Secunia #40268

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Jul 27, 2010 12:00:00 EDT

Patch Publication Date: Jul 22, 2010 12:00:00 EDT

Plugin Publication Date: Aug 4, 2010 12:00:00 EDT

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.13

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
Apache HTTP Server Byte Range DoS	High	10.3.0.122	443	TCP	Yes

Synopsis: The web server running on the remote host is affected by a denial of service vulnerability.

Description: The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive.

Exploit code is publicly available and attacks have reportedly been observed in the wild.

Solution: Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.

If the host is running a web server based on Apache httpd, contact the vendor for a fix.

See Also: http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html
http://www.gossamer-threads.com/lists/apache/dev/401638
http://www.nessus.org/u?404627ec
http://httpd.apache.org/security/CVE-2011-3192.txt
http://www.nessus.org/u?1538124a
http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Risk Factor: High

CVSS Base Score: 7.8

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C

CVSS Temporal Score: 6.4

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

-------------------- Testing for workarounds --------------------
HEAD / HTTP/1.1
Host: telmaxdr.victrackad.victrack.com.au
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
```

```
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.0 206 Partial Content
Date: Mon, 04 Nov 2013 14:29:05 GMT
Server: Apache/2.2.6 (Unix) DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Last-Modified: Wed, 19 May 2010 14:04:01 GMT
ETag: "1e23f-b9-ee0ed640"
Accept-Ranges: bytes
Content-Length: 826
Connection: close
Content-Type: multipart/x-byteranges; boundary=4ea5abd0346918fc
-------------------- Testing for workarounds --------------------

-------------------- Testing for patch --------------------
HEAD / HTTP/1.1
Host: telmaxdr.victrackad.victrack.com.au
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=0-,1-
Range: bytes=0-,1-
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.0 206 Partial Content
Date: Mon, 04 Nov 2013 14:29:05 GMT
Server: Apache/2.2.6 (Unix) DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Last-Modified: Wed, 19 May 2010 14:04:01 GMT
ETag: "1e23f-b9-ee0ed640"
Accept-Ranges: bytes
Content-Length: 558
Connection: close
Content-Type: multipart/x-byteranges; boundary=4ea5abd040dcc3b26
-------------------- Testing for patch --------------------
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3192

BID: 49303

Crossref: OSVDB #74721, CERT #405811, EDB-ID #17696, EDB-ID #18221

Vulnerability Publication Date: 2011/08/19

Patch Publication Date: 2011/08/25

Plugin Publication Date: 2011/08/25

Plugin Modification Date: 2012/10/16

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_range_dos.nasl
Synopsis: The web server running on the remote host is affected by a denial of service vulnerability.
Description: The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive. Exploit code is publicly available and attacks have reportedly been observed in the wild.
Solution: Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression. If the host is running a web server based on Apache httpd, contact the vendor for a fix.
See Also: http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html http://www.gossamer-threads.com/lists/apache/dev/401638 http://www.nessus.org/u?404627ec http://httpd.apache.org/security/CVE-2011-3192.txt http://www.nessus.org/u?1538124a http://www-01.ibm.com/support/docview.wss?uid=swg24030863
Risk Factor: High
STIG Severity:
CVSS Base Score: 7.8
CVSS Temporal Score: 6.4
CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C
CPE: cpe:/a:apache:http_server
CVE: CVE-2011-3192
BID: 49303
Cross References: OSVDB #74721,CERT #405811,EDB-ID #17696,EDB-ID #18221
First Discovered: Oct 3, 2011 12:05:54 EDT
Last Observed: Nov 4, 2013 10:37:50 EST
Vuln Publication Date: Aug 19, 2011 12:00:00 EDT
Patch Publication Date: Aug 25, 2011 12:00:00 EDT
Plugin Publication Date: Aug 25, 2011 12:00:00 EDT
Plugin Modification Date: Oct 16, 2012 12:00:00 EDT
Exploit Ease: Exploits are available
Exploit Frameworks: Metasploit (Apache Range header DoS (Apache Killer)), Core Impact
Check Type: remote
Version: Revision: 1.23

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.3.9 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes
Synopsis : The remote web server uses a version of PHP that is affected by multiple flaws. Description : According to its banner, the version of PHP installed on the remote host is older than 5.3.9. Such versions may be affected by several security issues :					

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

- An Integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

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

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

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

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

See also :

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

Solution :

Upgrade to PHP version 5.3.9 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.3.9
```

CVE : CVE-2011-4566, CVE-2011-4885, CVE-2012-0057, CVE-2012-0781, CVE-2012-0788, CVE-2012-0789
BID : 50907, 51193, 51806, 51952, 51992, 52043
Other references : OSVDB:77446, OSVDB:78115, OSVDB:78571, OSVDB:78676, OSVDB:79016

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

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

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

- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)
- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

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

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

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

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

Solution: Upgrade to PHP version 5.3.9 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.2

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2011-3379,CVE-2011-4566,CVE-2011-4885,CVE-2012-0057,CVE-2012-0788,CVE-2012-0781,CVE-2012-0789

BID: 50907,51193,51806,51992,51952,52043,49754

Cross References: OSVDB #77446,OSVDB #78115,OSVDB #78571,OSVDB #78676,OSVDB #79016,OSVDB #75713,OSVDB #79332

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Sep 23, 2011 12:00:00 EDT

Patch Publication Date: Jan 11, 2012 12:00:00 EST

Plugin Publication Date: Jan 13, 2012 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.14

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.3.11 Multiple Vulnerabilities	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

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

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

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

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

See also :

http://www.nessus.org/u?e81d4026
https://bugs.php.net/bug.php?id=61043
https://bugs.php.net/bug.php?id=54374
http://www.php.net/archive/2012.php#id2012-04-26-1
http://www.php.net/ChangeLog-5.php#5.3.11

Solution :

Upgrade to PHP version 5.3.11 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.3.11
```

CVE : CVE-2012-0831, CVE-2012-1172
BID : 51954, 53403
Other references : OSVDB:79017

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

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

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

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

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

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

Solution: Upgrade to PHP version 5.3.11 or later.

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

Risk Factor: High

STIG Severity:

CVSS Base Score: 7.5

CVSS Temporal Score: 6.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:ND/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2012-0831,CVE-2012-1172,CVE-2011-1398

BID: 51954,53403,55297

Cross References: OSVDB #79017,OSVDB #81791,OSVDB #85086

First Discovered: Jun 4, 2012 13:23:44 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Feb 9, 2012 12:00:00 EST

Patch Publication Date: Apr 26, 2012 12:00:00 EDT

Plugin Publication Date: May 2, 2012 12:00:00 EDT

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP Unsupported Version Detection	High	10.3.0.122	8457	TCP	No

Synopsis :

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

Description :

According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

See also :

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

Solution :

Upgrade to a version of PHP that is currently supported.

Risk factor :

Critical / CVSS Base Score : 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin output :

```
Source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
End of support date : 2011/12/16
Announcement : http://www.php.net/archive/2010.php
Supported versions : 5.3.x / 5.4.x
```

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

Description: According to its version, the installation of PHP on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution: Upgrade to a version of PHP that is currently supported.

See Also: https://wiki.php.net/rfc/releaseprocess

Risk Factor: Critical

STIG Severity:

CVSS Base Score: 10.0

CVSS Temporal Score:

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

CPE: cpe:/a:php:php

CVE:

BID:

Cross References:

First Discovered: Jun 4, 2012 13:23:44 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: May 4, 2012 12:00:00 EDT

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease:

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.3

Plugin Name	Severity	IP Address	Port	Protocol	Exploit?
PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	High	10.3.0.122	8457	TCP	Yes

Synopsis :

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

Description :

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

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

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

See also :

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

Solution :

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

Risk factor :

High / CVSS Base Score : 8.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P)
CVSS Temporal Score : 6.9
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.3.12 / 5.4.2
```

CVE : CVE-2012-1823
BID : 53388
Other references : OSVDB:81633, CERT-VU:520827

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

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

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

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

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

See Also: http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-03-1 http://www.php.net/ChangeLog-5.php#5.3.12 http://www.php.net/ChangeLog-5.php#5.4.2
Risk Factor: High
STIG Severity:
CVSS Base Score: 8.3
CVSS Temporal Score: 7.2
CVSS Vector: AV:N/AC:M/Au:N/C:C/I:P/A:P/E:ND/RL:OF/RC:C
CPE: cpe:/a:php:php
CVE: CVE-2012-1823
BID: 53388
Cross References: OSVDB #81633,CERT #520827
First Discovered: Jun 4, 2012 13:23:44 EDT
Last Observed: Jul 2, 2012 13:28:13 EDT
Vuln Publication Date: May 3, 2012 12:00:00 EDT
Patch Publication Date: May 3, 2012 12:00:00 EDT
Plugin Publication Date: May 4, 2012 12:00:00 EDT
Plugin Modification Date: Oct 30, 2013 12:00:00 EDT
Exploit Ease: Exploits are available
Exploit Frameworks: Canvas (CANVAS), Metasploit (PHP CGI Argument Injection), Core Impact
Check Type: remote
Version: Revision: 1.10

Details - Medium Vulnerabilities

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
HTTP TRACE / TRACK Methods Allowed	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: Debugging functions are enabled on the remote web server.

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

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

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

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.9

CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:C

Plugin Output:

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

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

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

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1863829314.html HTTP/1.1
Connection: Close
Host: telmaxdr.victrackad.victrack.com.au
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

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

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 04 Nov 2013 14:28:31 GMT
Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1863829314.html HTTP/1.1
Connection: Keep-Alive
Host: telmaxdr.victrackad.victrack.com.au
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

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

CVE: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386

BID: 9506, 9561, 11604, 33374, 37995

Crossref: OSVDB #877, OSVDB #3726, OSVDB #5648, OSVDB #50485, CERT #288308, CERT #867593, CWE #16

Vulnerability Publication Date: 2003/01/20

Plugin Publication Date: 2003/01/23

Plugin Modification Date: 2013/03/29

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: xst_http_trace.nasl

Synopsis: Debugging functions are enabled on the remote web server.

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

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

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.9

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:W/RC:C

CPE:

CVE: CVE-2004-2320,CVE-2003-1567,CVE-2010-0386

BID: 9506,9561,11604,33374,37995

Cross References: OSVDB #3726,OSVDB #50485,OSVDB #877,CWE #16,OSVDB #5648,CERT #288308,CERT #867593

First Discovered: Nov 14, 2010 22:26:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 20, 2003 12:00:00 EST

Patch Publication Date: N/A

Plugin Publication Date: Jan 23, 2003 12:00:00 EST

Plugin Modification Date: Mar 29, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (HTTP Options Detection)

Check Type: remote

Version: Revision: 1.59

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:ND

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Crossref: OSVDB #45420, CWE #79

Vulnerability Publication Date: 2008/05/08

Patch Publication Date: 2008/01/02

Plugin Publication Date: 2011/11/18

Plugin Modification Date: 2012/06/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_utf7_xss.nasl

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:ND

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Cross References: CWE #79,OSVDB #45420

First Discovered: Dec 5, 2011 11:13:24 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 8, 2008 12:00:00 EDT

Patch Publication Date: Jan 2, 2008 12:00:00 EST

Plugin Publication Date: Nov 18, 2011 12:00:00 EST

Plugin Modification Date: Jun 18, 2012 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.3

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:ND

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Crossref: OSVDB #45420, CWE #79

Vulnerability Publication Date: 2008/05/08

Patch Publication Date: 2008/01/02

Plugin Publication Date: 2011/11/18

Plugin Modification Date: 2012/06/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_utf7_xss.nasl

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:ND

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Cross References: CWE #79,OSVDB #45420

First Discovered: Dec 5, 2011 11:13:24 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 8, 2008 12:00:00 EDT

Patch Publication Date: Jan 2, 2008 12:00:00 EST

Plugin Publication Date: Nov 18, 2011 12:00:00 EST

Plugin Modification Date: Jun 18, 2012 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.3

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html
http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:ND

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Crossref: OSVDB #45420, CWE #79

Vulnerability Publication Date: 2008/05/08

Patch Publication Date: 2008/01/02

Plugin Publication Date: 2011/11/18

Plugin Modification Date: 2012/06/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_utf7_xss.nasl

Synopsis: The web server running on the remote host has a cross-site scripting vulnerability.

Description: According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

Solution: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

See Also: http://archives.neohapsis.com/archives/bugtraq/2008-05/0122.html http://archives.neohapsis.com/archives/bugtraq/2008-05/0184.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:ND

CPE: cpe:/a:apache:http_server

CVE: CVE-2008-2168

BID: 29112

Cross References: CWE #79,OSVDB #45420

First Discovered: Dec 5, 2011 11:13:24 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 8, 2008 12:00:00 EDT

Patch Publication Date: Jan 2, 2008 12:00:00 EST

Plugin Publication Date: Nov 18, 2011 12:00:00 EST

Plugin Modification Date: Jun 18, 2012 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.3

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.8 Multiple Vulnerabilit (XSS, DoS)	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005

BID: 26663, 26838, 27234, 27236, 27237

Crossref: OSVDB #39003, OSVDB #39133, OSVDB #39134, OSVDB #40262, OSVDB #40263, OSVDB #40264, OSVDB #42214, OSVDB #42937, CWE #79

Vulnerability Publication Date: 2007/11/14

Plugin Publication Date: 2008/02/20

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_8.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000,CVE-2007-6388,CVE-2007-6421,CVE-2007-6422,CVE-2008-0005,CVE-2007-6203

BID: 26663,26838,27234,27236,27237

Cross References: OSVDB #39003,OSVDB #39134,OSVDB #40262,OSVDB #40263,OSVDB #40264,OSVDB #42214,OSVDB #42937,CWE #79,OSVDB #39133

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Nov 14, 2007 12:00:00 EST

Patch Publication Date: N/A

Plugin Publication Date: Feb 20, 2008 12:00:00 EST

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.27

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.8 Multiple Vulnerabilit (XSS, DoS)	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005

BID: 26663, 26838, 27234, 27236, 27237

Crossref: OSVDB #39003, OSVDB #39133, OSVDB #39134, OSVDB #40262, OSVDB #40263, OSVDB #40264, OSVDB #42214, OSVDB #42937, CWE #79

Vulnerability Publication Date: 2007/11/14

Plugin Publication Date: 2008/02/20

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_8.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000,CVE-2007-6388,CVE-2007-6421,CVE-2007-6422,CVE-2008-0005,CVE-2007-6203

BID: 26663,26838,27234,27236,27237

Cross References: OSVDB #39003,OSVDB #39134,OSVDB #40262,OSVDB #40263,OSVDB #40264,OSVDB #42214,OSVDB #42937,CWE #79,OSVDB #39133

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Nov 14, 2007 12:00:00 EST

Patch Publication Date: N/A

Plugin Publication Date: Feb 20, 2008 12:00:00 EST

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.27

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.8 Multiple Vulnerabilit (XSS, DoS)	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.8
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000, CVE-2007-6203, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422, CVE-2008-0005

BID: 26663, 26838, 27234, 27236, 27237

Crossref: OSVDB #39003, OSVDB #39133, OSVDB #39134, OSVDB #40262, OSVDB #40263, OSVDB #40264, OSVDB #42214, OSVDB #42937, CWE #79

Vulnerability Publication Date: 2007/11/14

Plugin Publication Date: 2008/02/20

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_8.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.8. Such versions may be affected by several issues, including :

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

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

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

- A cross-site scripting issue in mod_proxy_balancer involving the worker route and worker redirect string of the balancer manager (CVE-2007-6421).

- A denial of service issue in the balancer_handler function in mod_proxy_balancer can be triggered by an authenticated user when a threaded Multi- Processing Module is used (CVE-2007-6422).

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.8 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-5000,CVE-2007-6388,CVE-2007-6421,CVE-2007-6422,CVE-2008-0005,CVE-2007-6203

BID: 26663,26838,27234,27236,27237

Cross References: OSVDB #39003,OSVDB #39134,OSVDB #40262,OSVDB #40263,OSVDB #40264,OSVDB #42214,OSVDB #42937,CWE #79,OSVDB #39133

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Nov 14, 2007 12:00:00 EST

Patch Publication Date: N/A

Plugin Publication Date: Feb 20, 2008 12:00:00 EST

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.27

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.9 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

(DoS,
XSS)

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http. (CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version Source : Server: Apache/2.2.6
Installed Version : 2.2.6
Fixed Version : 2.2.9
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420, CVE-2008-2364, CVE-2007-6423

BID: 27236, 29653

Crossref: OSVDB #42937, OSVDB #46085, Secunia #30621, CWE #399

Plugin Publication Date: 2008/07/11

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_9.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http. (CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420,CVE-2007-6423,CVE-2008-2364

BID: 27236,29653

Cross References: OSVDB #42937,OSVDB #46085,CWE #399,Secunia #30621

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Jul 11, 2008 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.29

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.9 Multiple Vulnerabilit (DoS, XSS)	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http. (CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer.
(CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version Source : Server: Apache/2.2.6
Installed Version : 2.2.6
Fixed Version : 2.2.9
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420, CVE-2008-2364, CVE-2007-6423

BID: 27236, 29653

Crossref: OSVDB #42937, OSVDB #46085, Secunia #30621, CWE #399

Plugin Publication Date: 2008/07/11

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_9.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http.
(CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer.
(CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420,CVE-2007-6423,CVE-2008-2364

BID: 27236,29653

Cross References: OSVDB #42937,OSVDB #46085,CWE #399,Secunia #30621

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Jul 11, 2008 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.29

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache < 2.2.9 Multiple Vulnerabilit (DoS, XSS)	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http. (CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer. (CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version Source : Server: Apache/2.2.6
Installed Version : 2.2.6
Fixed Version : 2.2.9
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420, CVE-2008-2364, CVE-2007-6423

BID: 27236, 29653

Crossref: OSVDB #42937, OSVDB #46085, Secunia #30621, CWE #399

Plugin Publication Date: 2008/07/11

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_9.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.9. Such versions may be affected by several issues, including :

- Improper handling of excessive forwarded interim responses may cause denial of service conditions in mod_proxy_http.
(CVE-2008-2364)

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer.
(CVE-2007-6420)

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.9 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2007-6420,CVE-2007-6423,CVE-2008-2364

BID: 27236,29653

Cross References: OSVDB #42937,OSVDB #46085,CWE #399,Secunia #30621

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Jul 11, 2008 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.29

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP < 5.2.9 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)

- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.

- Function 'explode()' is affected by an unspecified vulnerability.

- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.

- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See also :

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

Solution :

Upgrade to PHP version 5.2.9 or later.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS Temporal Score : 4.1
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.9

CVE : CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID : 33002, 33927
Other references : OSVDB:51031, OSVDB:52486, OSVDB:53440, Secunia:34081, CWE:200

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

Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)

- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.

- Function 'explode()' is affected by an unspecified vulnerability.

- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.

- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

Solution: Upgrade to PHP version 5.2.9 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2008-5498,CVE-2009-1271,CVE-2009-1272

BID: 33002,33927

Cross References: CWE #200,OSVDB #51031,OSVDB #52486,OSVDB #53440,Secunia #34081

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: N/A

Patch Publication Date: Feb 26, 2009 12:00:00 EST

Plugin Publication Date: Feb 27, 2009 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.11

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP < 5.2.10 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

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

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

See also :

http://bugs.php.net/bug.php?id=45997
http://bugs.php.net/bug.php?id=48378
http://www.php.net/releases/5_2_10.php
http://www.php.net/ChangeLog-5.php#5.2.10

Solution :

Upgrade to PHP version 5.2.10 or later.

Risk factor :

Medium / CVSS Base Score : 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 4.8
(CVSS2#E:F/RL:U/RC:C)
Public Exploit Available : true

Plugin output :

```
Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.10
```

CVE : CVE-2009-2687

BID : 35440, 35435
Other references : OSVDB:55222, OSVDB:55223, OSVDB:55224, Secunia:35441, CWE:20

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

Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

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

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

Solution: Upgrade to PHP version 5.2.10 or later.

See Also: http://bugs.php.net/bug.php?id=45997
http://bugs.php.net/bug.php?id=48378
http://www.php.net/releases/5_2_10.php
http://www.php.net/ChangeLog-5.php#5.2.10

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.1

CVSS Temporal Score: 4.8

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:U/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2009-2687

BID: 35435,35440

Cross References: OSVDB #55222,OSVDB #55224,CWE #20,OSVDB #55223,Secunia #35441

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: May 24, 2009 12:00:00 EDT

Patch Publication Date: Jun 18, 2009 12:00:00 EDT

Plugin Publication Date: Jun 22, 2009 12:00:00 EDT

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.x < 2.2.12 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (&gt;10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSS Temporal Score: 4.7

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.12
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956

BID: 34663, 35115, 35221, 35251, 35253, 35565, 35623

Crossref: OSVDB #53921, OSVDB #54733, OSVDB #55057, OSVDB #55058, OSVDB #55059, OSVDB #55553, OSVDB #55782, CWE #119

Vulnerability Publication Date: 2009/04/22

Patch Publication Date: 2009/07/27

Plugin Publication Date: 2009/08/02

Plugin Modification Date: 2013/07/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_12.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score: 4.7

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-1890,CVE-2009-1891,CVE-2009-0023,CVE-2009-1955,CVE-2009-1956,CVE-2009-1195,CVE-2009-1191

BID: 35565,35623,35221,35115,34663,35251,35253

Cross References: OSVDB #54733,OSVDB #55553,OSVDB #55059,CWE #119,OSVDB #55057,OSVDB #55058,OSVDB #53921,OSVDB #55782

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Apr 22, 2009 12:00:00 EDT

Patch Publication Date: Jul 27, 2009 12:00:00 EDT

Plugin Publication Date: Aug 2, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.15

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.x < 2.2.12 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (&gt;10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSS Temporal Score: 4.7

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.12

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956

BID: 34663, 35115, 35221, 35251, 35253, 35565, 35623

Crossref: OSVDB #53921, OSVDB #54733, OSVDB #55057, OSVDB #55058, OSVDB #55059, OSVDB #55553, OSVDB #55782, CWE #119

Vulnerability Publication Date: 2009/04/22

Patch Publication Date: 2009/07/27

Plugin Publication Date: 2009/08/02

Plugin Modification Date: 2013/07/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_12.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score: 4.7

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-1890,CVE-2009-1891,CVE-2009-0023,CVE-2009-1955,CVE-2009-1956,CVE-2009-1195,CVE-2009-1191

BID: 35565,35623,35221,35115,34663,35251,35253

Cross References: OSVDB #54733,OSVDB #55553,OSVDB #55059,CWE #119,OSVDB #55057,OSVDB #55058,OSVDB #53921,OSVDB #55782

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Apr 22, 2009 12:00:00 EDT

Patch Publication Date: Jul 27, 2009 12:00:00 EDT

Plugin Publication Date: Aug 2, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.15

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.x < 2.2.12 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (&gt;10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSS Temporal Score: 4.7

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.12
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-0023, CVE-2009-1191, CVE-2009-1195, CVE-2009-1890, CVE-2009-1891, CVE-2009-1955, CVE-2009-1956

BID: 34663, 35115, 35221, 35251, 35253, 35565, 35623

Crossref: OSVDB #53921, OSVDB #54733, OSVDB #55057, OSVDB #55058, OSVDB #55059, OSVDB #55553, OSVDB #55782, CWE #119

Vulnerability Publication Date: 2009/04/22

Patch Publication Date: 2009/07/27

Plugin Publication Date: 2009/08/02

Plugin Modification Date: 2013/07/20

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_12.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.12. Such versions may be affected by several issues, including :

- A heap buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon. (CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body. (CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

Solution: Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score: 4.7

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-1890,CVE-2009-1891,CVE-2009-0023,CVE-2009-1955,CVE-2009-1956,CVE-2009-1195,CVE-2009-1191

BID: 35565,35623,35221,35115,34663,35251,35253

Cross References: OSVDB #54733,OSVDB #55553,OSVDB #55059,CWE #119,OSVDB #55057,OSVDB #55058,OSVDB #53921,OSVDB #55782

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Apr 22, 2009 12:00:00 EDT

Patch Publication Date: Jul 27, 2009 12:00:00 EDT

Plugin Publication Date: Aug 2, 2009 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.15

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
NTP ntpd Mode 7 Error Response Packet Loop	Medium	10.3.0.122	REP_CIT	123	UDP	Misc.	Yes

Remote
DoS

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote network time service has a denial of service vulnerability.

Description: The version of ntpd running on the remote host has a denial of service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.

Solution: Upgrade to NTP 4.2.4p8 / 4.2.6 or later.

See Also: https://support.ntp.org/bugs/show_bug.cgi?id=1331
http://www.nessus.org/u?3a07ed05

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P

CVSS Temporal Score: 5.3

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVE: CVE-2009-3563

BID: 37255

Crossref: OSVDB #60847, CERT #568372, Secunia #37629

Vulnerability Publication Date: 2009/11/04

Patch Publication Date: 2009/12/08

Plugin Publication Date: 2009/12/14

Plugin Modification Date: 2012/08/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: ntpd_mode7_ping_pong_dos.nasl

Synopsis: The remote network time service has a denial of service vulnerability.

Description: The version of ntpd running on the remote host has a denial of service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.

Solution: Upgrade to NTP 4.2.4p8 / 4.2.6 or later.

See Also: https://support.ntp.org/bugs/show_bug.cgi?id=1331
http://www.nessus.org/u?3a07ed05

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score: 5.3

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:P/E:F/RL:OF/RC:C

CPE:

CVE: CVE-2009-3563

BID: 37255

Cross References: OSVDB #60847,CERT #568372,Secunia #37629

First Discovered: Mar 4, 2013 10:04:55 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Nov 4, 2009 12:00:00 EST

Patch Publication Date: Dec 8, 2009 12:00:00 EST

Plugin Publication Date: Dec 14, 2009 12:00:00 EST

Plugin Modification Date: Aug 15, 2012 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (NTP.org ntpd Reserved Mode Denial of Service)

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP < 5.2.12 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)

- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, he may be able to cause the web server to stop responding while it processes the file list. (CVE-2009-4017)

- Missing protection for '$_SESSION' from interrupt corruption and improved 'session.save_path' check.

(CVE-2009-4143)

- Insufficient input string validation in the
'htmlspecialchars()' function. (CVE-2009-4142)

See also :

http://www.nessus.org/u?57f2d08f
http://www.php.net/releases/5_2_12.php
http://www.php.net/ChangeLog-5.php#5.2.12

Solution :

Upgrade to PHP version 5.2.12 or later.

Risk factor :

Medium / CVSS Base Score : 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.6
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.12

CVE : CVE-2009-3557, CVE-2009-3558, CVE-2009-4017, CVE-2009-4142, CVE-2009-4143
BID : 37389, 37390
Other references : OSVDB:60434, OSVDB:60435, OSVDB:60451, OSVDB:61208, OSVDB:61209, Secunia:37821, CWE:264

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

Description: According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)

- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list. (CVE-2009-4017)

- Missing protection for '$_SESSION' from interrupt corruption and improved 'session.save_path' check.
(CVE-2009-4143)

- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

Solution: Upgrade to PHP version 5.2.12 or later.

See Also: http://www.nessus.org/u?57f2d08f
http://www.php.net/releases/5_2_12.php
http://www.php.net/ChangeLog-5.php#5.2.12

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.8

CVSS Temporal Score: 5.6

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2009-3557,CVE-2009-3558,CVE-2009-4017,CVE-2009-4142,CVE-2009-4143

BID: 37389,37390

Cross References: OSVDB #60434,OSVDB #60435,OSVDB #61208,OSVDB #61209,OSVDB #60451,CWE #264,Secunia #37821

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Dec 17, 2009 12:00:00 EST

Patch Publication Date: Dec 17, 2009 12:00:00 EST

Plugin Publication Date: Dec 18, 2009 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.13

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

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

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

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

- An unspecified vulnerability affects the LCG entropy.

See also :

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

Solution :

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk factor :

Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
CVSS Temporal Score : 5.3
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.3.2 / 5.2.13

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

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

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

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

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

- An unspecified vulnerability affects the LCG entropy.

Solution: Upgrade to PHP version 5.3.2 / 5.2.13 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score: 5.3

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2010-1128,CVE-2010-1129,CVE-2010-1130

BID: 38182,38430,38431

Cross References: OSVDB #62582,OSVDB #62583,OSVDB #63323,Secunia #38708

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Feb 11, 2010 12:00:00 EST

Patch Publication Date: Feb 25, 2010 12:00:00 EST

Plugin Publication Date: Feb 26, 2010 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.11

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.16 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.16

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452, CVE-2010-2068

BID: 40827, 41963

Crossref: OSVDB #65654, OSVDB #66745, Secunia #40206

Vulnerability Publication Date: 2010/06/11

Patch Publication Date: 2010/07/25

Plugin Publication Date: 2010/07/30

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_16.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452,CVE-2010-2068

BID: 40827,41963

Cross References: OSVDB #65654,OSVDB #66745,Secunia #40206

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jun 11, 2010 12:00:00 EDT

Patch Publication Date: Jul 25, 2010 12:00:00 EDT

Plugin Publication Date: Jul 30, 2010 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.20

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.16 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.16
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452, CVE-2010-2068

BID: 40827, 41963

Crossref: OSVDB #65654, OSVDB #66745, Secunia #40206

Vulnerability Publication Date: 2010/06/11

Patch Publication Date: 2010/07/25

Plugin Publication Date: 2010/07/30

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_16.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452,CVE-2010-2068

BID: 40827,41963

Cross References: OSVDB #65654,OSVDB #66745,Secunia #40206

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jun 11, 2010 12:00:00 EDT

Patch Publication Date: Jul 25, 2010 12:00:00 EDT

Plugin Publication Date: Jul 30, 2010 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.20

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.16 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

- A denial of service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.16

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452, CVE-2010-2068

BID: 40827, 41963

Crossref: OSVDB #65654, OSVDB #66745, Secunia #40206

Vulnerability Publication Date: 2010/06/11

Patch Publication Date: 2010/07/25

Plugin Publication Date: 2010/07/30

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_16.nasl

Synopsis: The remote web server is affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.16. Such versions are potentially affected by multiple vulnerabilities :

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

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

Solution: Upgrade to Apache version 2.2.16 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2010-1452,CVE-2010-2068

BID: 40827,41963

Cross References: OSVDB #65654,OSVDB #66745,Secunia #40206

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jun 11, 2010 12:00:00 EDT

Patch Publication Date: Jul 25, 2010 12:00:00 EDT

Plugin Publication Date: Jul 30, 2010 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.20

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.17 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.17
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3560, CVE-2009-3720, CVE-2010-1623

BID: 37203, 36097, 43673

Crossref: OSVDB #59737, OSVDB #60797, OSVDB #68327, Secunia #41701, CWE #119

Vulnerability Publication Date: 2009/01/17

Patch Publication Date: 2010/10/19

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/04/26

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_17.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3720,CVE-2009-3560,CVE-2010-1623

BID: 43673,37203,36097

Cross References: CWE #119,OSVDB #59737,OSVDB #60797,OSVDB #68327,Secunia #41701

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 17, 2009 12:00:00 EST

Patch Publication Date: Oct 19, 2010 12:00:00 EDT

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Apr 26, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.9

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.17 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6

Installed version : 2.2.6
Fixed version : 2.2.17

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3560, CVE-2009-3720, CVE-2010-1623

BID: 37203, 36097, 43673

Crossref: OSVDB #59737, OSVDB #60797, OSVDB #68327, Secunia #41701, CWE #119

Vulnerability Publication Date: 2009/01/17

Patch Publication Date: 2010/10/19

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/04/26

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_17.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3720,CVE-2009-3560,CVE-2010-1623

BID: 43673,37203,36097

Cross References: CWE #119,OSVDB #59737,OSVDB #60797,OSVDB #68327,Secunia #41701

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 17, 2009 12:00:00 EST

Patch Publication Date: Oct 19, 2010 12:00:00 EDT

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Apr 26, 2013 12:00:00 EDT
Exploit Ease: Exploits are available
Exploit Frameworks:
Check Type: remote
Version: Revision: 1.9

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.17 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.17

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3560, CVE-2009-3720, CVE-2010-1623

BID: 37203, 36097, 43673

Crossref: OSVDB #59737, OSVDB #60797, OSVDB #68327, Secunia #41701, CWE #119

Vulnerability Publication Date: 2009/01/17

Patch Publication Date: 2010/10/19

Plugin Publication Date: 2010/10/20

Plugin Modification Date: 2013/04/26

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_17.nasl

Synopsis: The remote web server may be affected by several issues.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.17. Such versions may be affected by several issues, including :

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.17 or later.

See Also: http://www.nessus.org/u?1c39fa1c
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2009-3720,CVE-2009-3560,CVE-2010-1623

BID: 43673,37203,36097

Cross References: CWE #119,OSVDB #59737,OSVDB #60797,OSVDB #68327,Secunia #41701

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 17, 2009 12:00:00 EST

Patch Publication Date: Oct 19, 2010 12:00:00 EDT

Plugin Publication Date: Oct 20, 2010 12:00:00 EDT

Plugin Modification Date: Apr 26, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.9

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP 5.2 < 5.2.15	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	No

Multiple
Vulnerabilit

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.15. Such versions may be affected by several security issues :

- A crash in the zip extract method.

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

- An unspecified flaw exists in 'open_basedir'. (CVE-2010-3436)

- A possible crash could occur in 'mssql_fetch_batch()'.

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

- A crash exists if anti-aliasing steps are invalid. (Bug #53492)

- A crash exists in pdo_firebird getAttribute(). (Bug #53323)

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

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

- The extract function does not prevent use of the EXTR_OVERWRITE parameter to overwrite the GLOBALS superglobal array and the 'this' variable, which allows attackers to bypass intended access restrictions. (CVE-2011-0752)

See also :

http://www.php.net/releases/5_2_15.php
http://www.php.net/ChangeLog-5.php#5.2.15

Solution :

Upgrade to PHP version 5.2.15 or later.

Risk factor :

Medium / CVSS Base Score : 6.8

```
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.0
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.15

CVE : CVE-2010-3436, CVE-2010-3709, CVE-2010-4150, CVE-2010-4697, CVE-2010-4698, CVE-2011-0752
BID : 44718, 44723, 45335, 45952, 46448
Other references : OSVDB:68597, OSVDB:69109, OSVDB:69110, OSVDB:69660, OSVDB:70607, OSVDB:70608, OSVDB:74728
```

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

Description: According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.15. Such versions may be affected by several security issues :

- A crash in the zip extract method.

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

- An unspecified flaw exists in 'open_basedir'. (CVE-2010-3436)

- A possible crash could occur in 'mssql_fetch_batch()'.

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

- A crash exists if anti-aliasing steps are invalid.
(Bug #53492)

- A crash exists in pdo_firebird getAttribute(). (Bug #53323)

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

- A stack-based buffer overflow exists in the 'imagepstext()' function in the GD extension. (Bug #53492 / CVE-2010-4698)
- The extract function does not prevent use of the EXTR_OVERWRITE parameter to overwrite the GLOBALS superglobal array and the 'this' variable, which allows attackers to bypass intended access restrictions.
(CVE-2011-0752)

Solution: Upgrade to PHP version 5.2.15 or later.

See Also: http://www.php.net/releases/5_2_15.php
http://www.php.net/ChangeLog-5.php#5.2.15

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.8

CVSS Temporal Score: 5.0

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P/E:U/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2010-3436,CVE-2010-3709,CVE-2010-4150,CVE-2010-4697,CVE-2010-4698,CVE-2011-0752

BID: 44718,44723,45335,45952,46448

Cross References: OSVDB #68597,OSVDB #69109,OSVDB #69110,OSVDB #69660,OSVDB #70607,OSVDB #70608,OSVDB #74728

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Dec 10, 2010 12:00:00 EST
Patch Publication Date: Dec 10, 2010 12:00:00 EST
Plugin Publication Date: Dec 13, 2010 12:00:00 EST
Plugin Modification Date: Oct 23, 2013 12:00:00 EDT
Exploit Ease: No known exploits are available
Exploit Frameworks:
Check Type: remote
Version: Revision: 1.13

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
SSL Certificate Cannot Be Trusted	Medium	10.3.0.122	REP_CIT	443	TCP	General	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The SSL certificate for this service cannot be trusted.

Description: The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution: Purchase or generate a proper certificate for this service.

Risk Factor: Medium

CVSS Base Score: 6.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Plugin Output:

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : C=AU/ST=Victoria/L=Melbourne/O=Victorian Rail Track/OU=IT/CN=telmax21.victrackad.victrack.com.au/
E=info@victrack.com.au
|-Issuer : DC=au/DC=com/DC=victrack/DC=victrackad/CN=victrackad-S-VM-CA02-CA
```

Plugin Publication Date: 2010/12/15

Plugin Modification Date: 2012/10/25

Plugin Type: remote

Source File: ssl_signed_certificate.nasl

Synopsis: The SSL certificate for this service cannot be trusted.

Description: The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain nullifies the use of SSL as anyone could establish a man-in-the- middle attack against the remote host.

Solution: Purchase or generate a proper certificate for this service.

See Also:

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.4

CVSS Temporal Score:

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

CPE:

CVE:

BID:

Cross References:

First Discovered: Jan 4, 2011 10:14:22 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Dec 15, 2010 12:00:00 EST

Plugin Modification Date: Oct 25, 2012 12:00:00 EDT

Exploit Ease:

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.12

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double	Medium	10.3.0.122	REP_CIT	8457	TCP	CGI abuses	Yes

Conversion
DoS

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis :

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

Description :

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

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

See also :

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

Solution :

Upgrade to PHP 5.2.17/5.3.5 or later.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS Temporal Score : 4.1
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

Plugin output :

Version source : Server: Apache/2.2.6 (Unix) PHP/5.2.5 DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e mod_perl/2.0.3 Perl/v5.8.8
Installed version : 5.2.5
Fixed version : 5.2.17/5.3.5

CVE : CVE-2010-4645
BID : 45668
Other references : OSVDB:70370

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

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

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

Solution: Upgrade to PHP 5.2.17/5.3.5 or later.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2010-4645

BID: 45668

Cross References: OSVDB #70370

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Jul 2, 2012 13:28:13 EDT

Vuln Publication Date: Dec 30, 2010 12:00:00 EST

Patch Publication Date: Jan 6, 2011 12:00:00 EST

Plugin Publication Date: Jan 7, 2011 12:00:00 EST

Plugin Modification Date: Oct 23, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.7

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
OpenSSL SSL_OP_N Ciphersuite Disabled Cipher Issue	Medium	10.3.0.122	REP_CIT	443	TCP	General	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote host allows the resumption of SSL sessions with a disabled cipher.

Description: The version of OpenSSL on the remote host has been shown to allow the use of disabled ciphers when resuming a session. This means that an attacker that sees (e.g. by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a disabled cipher chosen by the attacker.

Solution: Upgrade to OpenSSL 0.9.8j or later.

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.2

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:

```
The server allowed the following session over SSLv3 to be resumed as follows :

Session ID : 6a0331bb88b93dc0fb37b9e5b314537e2168c926b541a06973e3deaceb3ae534
Initial Cipher : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Resumed Cipher : SSL3_CK_EDH_DSS_DES_192_CBC3_SHA (0x0013)

CPE: cpe:/a:openssl:openssl

CVE: CVE-2008-7270

BID: 45254

Crossref: OSVDB #69655

Vulnerability Publication Date: 2010/12/02

Patch Publication Date: 2008/09/22

Plugin Publication Date: 2011/02/07

Plugin Modification Date: 2012/04/17

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: openssl_resume_disabled_cipher.nasl

Synopsis: The remote host allows the resumption of SSL sessions with a disabled cipher.

Description: The version of OpenSSL on the remote host has been shown to allow the use of disabled ciphers when resuming a session. This means that an attacker that sees (e.g. by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a disabled cipher chosen by the attacker.

Solution: Upgrade to OpenSSL 0.9.8j or later.

See Also:

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.2

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C

CPE: cpe:/a:openssl:openssl

CVE: CVE-2008-7270

BID: 45254

Cross References: OSVDB #69655

First Discovered: Aug 5, 2013 12:24:36 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Dec 2, 2010 12:00:00 EST

Patch Publication Date: Sep 22, 2008 12:00:00 EDT

Plugin Publication Date: Feb 7, 2011 12:00:00 EST

Plugin Modification Date: Apr 17, 2012 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.12

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.18 APR apr_fnmatc DoS	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.18
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Crossref: OSVDB #73388, Secunia #44574

Vulnerability Publication Date: 2011/05/10

Patch Publication Date: 2011/05/12

Plugin Publication Date: 2011/05/13

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_18.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Cross References: OSVDB #73388,Secunia #44574

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 10, 2011 12:00:00 EDT

Patch Publication Date: May 12, 2011 12:00:00 EDT

Plugin Publication Date: May 13, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.12

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.18 APR apr_fnmatc DoS	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.18
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Crossref: OSVDB #73388, Secunia #44574

Vulnerability Publication Date: 2011/05/10

Patch Publication Date: 2011/05/12

Plugin Publication Date: 2011/05/13

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_18.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Cross References: OSVDB #73388,Secunia #44574

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 10, 2011 12:00:00 EDT

Patch Publication Date: May 12, 2011 12:00:00 EDT

Plugin Publication Date: May 13, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.12

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.18 APR apr_fnmatc DoS	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f

http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.18
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Crossref: OSVDB #73388, Secunia #44574

Vulnerability Publication Date: 2011/05/10

Patch Publication Date: 2011/05/12

Plugin Publication Date: 2011/05/13

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_18.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.18. Such versions are affected by a denial of service vulnerability due to an error in the 'apr_fnmatch' match function of the bundled APR library.

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

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

Solution: Either ensure the 'IndexOptions' configuration option is set to 'IgnoreClient' or upgrade to Apache version 2.2.18 or later.

See Also: http://www.nessus.org/u?5582384f
http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18
http://securityreason.com/achievement_securityalert/98

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-0419

BID: 47820

Cross References: OSVDB #73388,Secunia #44574

First Discovered: Jun 6, 2011 12:11:59 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 10, 2011 12:00:00 EDT

Patch Publication Date: May 12, 2011 12:00:00 EDT

Plugin Publication Date: May 13, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.12

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.21 mod_proxy DoS	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.21

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Crossref: OSVDB #75647

Vulnerability Publication Date: 2011/09/14

Patch Publication Date: 2011/09/14

Plugin Publication Date: 2011/09/16

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_21.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Cross References: OSVDB #75647

First Discovered: Oct 3, 2011 12:05:54 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Sep 14, 2011 12:00:00 EDT

Patch Publication Date: Sep 14, 2011 12:00:00 EDT

Plugin Publication Date: Sep 16, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.21 mod_proxy DoS	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.21
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Crossref: OSVDB #75647

Vulnerability Publication Date: 2011/09/14

Patch Publication Date: 2011/09/14

Plugin Publication Date: 2011/09/16

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_21.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Cross References: OSVDB #75647

First Discovered: Oct 3, 2011 12:05:54 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Sep 14, 2011 12:00:00 EDT

Patch Publication Date: Sep 14, 2011 12:00:00 EDT

Plugin Publication Date: Sep 16, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.21 mod_proxy DoS	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.21
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Crossref: OSVDB #75647

Vulnerability Publication Date: 2011/09/14

Patch Publication Date: 2011/09/14

Plugin Publication Date: 2011/09/16

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_21.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.21. It therefore is potentially affected by a denial of service vulnerability.

An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

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

Solution: Upgrade to Apache version 2.2.21 or later.

See Also: http://www.nessus.org/u?34a2f1d8
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3348

BID: 49616

Cross References: OSVDB #75647

First Discovered: Oct 3, 2011 12:05:54 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Sep 14, 2011 12:00:00 EDT

Patch Publication Date: Sep 14, 2011 12:00:00 EDT

Plugin Publication Date: Sep 16, 2011 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
SMB Signing Disabled	Medium	10.3.0.122	REP_CIT	445	TCP	Misc.	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: Signing is disabled on the remote SMB server.

Description: Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

Solution: Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

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

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CPE: cpe:/o:microsoft:windows

Vulnerability Publication Date: 2012/01/17

Plugin Publication Date: 2012/01/19

Plugin Modification Date: 2013/10/24

Plugin Type: remote

Source File: smb_signing_disabled.nasl

Synopsis: Signing is disabled on the remote SMB server.

Description: Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

Solution: Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score:

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

CPE: cpe:/o:microsoft:windows

CVE:

BID:

Cross References:

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 17, 2012 12:00:00 EST

Patch Publication Date: N/A

Plugin Publication Date: Jan 19, 2012 12:00:00 EST

Plugin Modification Date: Oct 24, 2013 12:00:00 EDT

Exploit Ease:

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.22 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.22
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053, CVE-2012-4557

BID: 49957, 50494, 50802, 51407, 51705, 51706, 56753

Crossref: OSVDB #76079, OSVDB #76744, OSVDB #77310, OSVDB #78293, OSVDB #78555, OSVDB #78556, OSVDB #89275

Vulnerability Publication Date: 2011/10/05

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/06/03

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_22.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368,CVE-2011-4317,CVE-2011-3607,CVE-2012-0053,CVE-2012-0021,CVE-2012-0031,CVE-2012-4557

BID: 49957,50802,51706,50494,51407,51705,56753

Cross References: OSVDB #76079,OSVDB #76744,OSVDB #77310,OSVDB #78293,OSVDB #78555,OSVDB #78556,OSVDB #89275

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2011 12:00:00 EDT

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Jun 3, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache Reverse Proxy Bypass Vulnerability Scanner)

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 <	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

2.2.22
Multiple
Vulnerabilit

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.22
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053, CVE-2012-4557

BID: 49957, 50494, 50802, 51407, 51705, 51706, 56753

Crossref: OSVDB #76079, OSVDB #76744, OSVDB #77310, OSVDB #78293, OSVDB #78555, OSVDB #78556, OSVDB #89275

Vulnerability Publication Date: 2011/10/05

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/06/03

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_22.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368,CVE-2011-4317,CVE-2011-3607,CVE-2012-0053,CVE-2012-0021,CVE-2012-0031,CVE-2012-4557

BID: 49957,50802,51706,50494,51407,51705,56753

Cross References: OSVDB #76079,OSVDB #76744,OSVDB #77310,OSVDB #78293,OSVDB #78555,OSVDB #78556,OSVDB #89275

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2011 12:00:00 EDT

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Jun 3, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache Reverse Proxy Bypass Vulnerability Scanner)

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.22 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 4.1

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.22

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368, CVE-2011-3607, CVE-2011-4317, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053, CVE-2012-4557

BID: 49957, 50494, 50802, 51407, 51705, 51706, 56753

Crossref: OSVDB #76079, OSVDB #76744, OSVDB #77310, OSVDB #78293, OSVDB #78555, OSVDB #78556, OSVDB #89275

Vulnerability Publication Date: 2011/10/05

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/06/03

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_22.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

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

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

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

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

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

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

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

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://www.nessus.org/u?81e2eb5f

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

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 5.0

CVSS Temporal Score: 4.1

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2011-3368,CVE-2011-4317,CVE-2011-3607,CVE-2012-0053,CVE-2012-0021,CVE-2012-0031,CVE-2012-4557

BID: 49957,50802,51706,50494,51407,51705,56753

Cross References: OSVDB #76079,OSVDB #76744,OSVDB #77310,OSVDB #78293,OSVDB #78555,OSVDB #78556,OSVDB #89275

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Oct 5, 2011 12:00:00 EDT

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Jun 3, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks: Metasploit (Apache Reverse Proxy Bypass Vulnerability Scanner)

Check Type: remote

Version: Revision: 1.10

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server httpOnly Cookie Information Disclosure	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

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

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: telmaxdr.victrackad.victrack.com.au
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

&lt;!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"&gt;
&lt;html&gt;&lt;head&gt;
&lt;title&gt;400 Bad Request&lt;/title&gt;
&lt;/head&gt;&lt;body&gt;
&lt;h1&gt;Bad Request&lt;/h1&gt;
&lt;p&gt;Your browser sent a request that this server could not understand.&lt;br /&gt;
Size of a request header field exceeds server limit.&lt;br /&gt;
&lt;pre&gt;
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Crossref: OSVDB #78556, EDB-ID #18442

Vulnerability Publication Date: 2012/01/23

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/10/01

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_httponly_info_leak.nasl

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Cross References: OSVDB #78556,EDB-ID #18442

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 23, 2012 12:00:00 EST

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Oct 1, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.7

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server httpOnly Cookie Information Disclosure	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

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

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Nessus verified this by sending a request with a long Cookie header :

GET / HTTP/1.1
Host: telmaxdr.victrackad.victrack.com.au
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

&lt;!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"&gt;
&lt;html&gt;&lt;head&gt;
&lt;title&gt;400 Bad Request&lt;/title&gt;
&lt;/head&gt;&lt;body&gt;
&lt;h1&gt;Bad Request&lt;/h1&gt;
&lt;p&gt;Your browser sent a request that this server could not understand.&lt;br /&gt;
Size of a request header field exceeds server limit.&lt;br /&gt;
&lt;pre&gt;
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Crossref: OSVDB #78556, EDB-ID #18442

Vulnerability Publication Date: 2012/01/23

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/10/01

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_httponly_info_leak.nasl

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Cross References: OSVDB #78556,EDB-ID #18442

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 23, 2012 12:00:00 EST

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Oct 1, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.7

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache HTTP Server httpOnly Cookie Information Disclosure	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

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

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Nessus verified this by sending a request with a long Cookie header :

```
GET / HTTP/1.1
Host: telmaxdr.victrackad.victrack.com.au:8457
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

```
&lt;!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"&gt;
&lt;html&gt;&lt;head&gt;
&lt;title&gt;400 Bad Request&lt;/title&gt;
&lt;/head&gt;&lt;body&gt;
&lt;h1&gt;Bad Request&lt;/h1&gt;
&lt;p&gt;Your browser sent a request that this server could not understand.&lt;br /&gt;
Size of a request header field exceeds server limit.&lt;br /&gt;
&lt;pre&gt;
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Crossref: OSVDB #78556, EDB-ID #18442

Vulnerability Publication Date: 2012/01/23

Patch Publication Date: 2012/01/31

Plugin Publication Date: 2012/02/02

Plugin Modification Date: 2013/10/01

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_httponly_info_leak.nasl

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

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

Solution: Upgrade to Apache version 2.2.22 or later.

See Also: http://fd.the-wildcat.de/apache_e36a9cf46c.php

http://httpd.apache.org/security/vulnerabilities_22.html
http://svn.apache.org/viewvc?view=revision&revision=1235454

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0053

BID: 51706

Cross References: OSVDB #78556,EDB-ID #18442

First Discovered: Feb 6, 2012 10:20:49 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Jan 23, 2012 12:00:00 EST

Patch Publication Date: Jan 31, 2012 12:00:00 EST

Plugin Publication Date: Feb 2, 2012 12:00:00 EST

Plugin Modification Date: Oct 1, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.7

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.23 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 6.9

CVSS Vector: CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.23
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883, CVE-2012-2687

BID: 53046, 55131

Crossref: OSVDB #81359, OSVDB #84818

Vulnerability Publication Date: 2012/03/02

Patch Publication Date: 2012/09/13

Plugin Publication Date: 2012/09/14

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_23.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.9

CVSS Temporal Score: 5.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883,CVE-2012-2687

BID: 53046,55131

Cross References: OSVDB #81359,OSVDB #84818

First Discovered: Feb 4, 2013 10:05:13 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 2, 2012 12:00:00 EST

Patch Publication Date: Sep 13, 2012 12:00:00 EDT

Plugin Publication Date: Sep 14, 2012 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.6

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.23 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 6.9

CVSS Vector: CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.23
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883, CVE-2012-2687

BID: 53046, 55131

Crossref: OSVDB #81359, OSVDB #84818

Vulnerability Publication Date: 2012/03/02

Patch Publication Date: 2012/09/13

Plugin Publication Date: 2012/09/14

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_23.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.9

CVSS Temporal Score: 5.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883,CVE-2012-2687

BID: 53046,55131

Cross References: OSVDB #81359,OSVDB #84818

First Discovered: Feb 4, 2013 10:05:13 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 2, 2012 12:00:00 EST

Patch Publication Date: Sep 13, 2012 12:00:00 EDT

Plugin Publication Date: Sep 14, 2012 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.6

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.23 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 6.9

CVSS Vector: CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Score: 5.7

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.23
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883, CVE-2012-2687

BID: 53046, 55131

Crossref: OSVDB #81359, OSVDB #84818

Vulnerability Publication Date: 2012/03/02

Patch Publication Date: 2012/09/13

Plugin Publication Date: 2012/09/14

Plugin Modification Date: 2013/07/20

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_23.nasl

Synopsis: The remote web server may be affected by multiple vulnerabilities.

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.23. It is, therefore, potentially affected by the following vulnerabilities:

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

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

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

Solution: Upgrade to Apache version 2.2.23 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.23
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 6.9

CVSS Temporal Score: 5.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-0883,CVE-2012-2687

BID: 53046,55131

Cross References: OSVDB #81359,OSVDB #84818

First Discovered: Feb 4, 2013 10:05:13 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Mar 2, 2012 12:00:00 EST

Patch Publication Date: Sep 13, 2012 12:00:00 EDT

Plugin Publication Date: Sep 14, 2012 12:00:00 EDT

Plugin Modification Date: Jul 20, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.6

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
TLS CRIME Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	General	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

Synopsis: The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description: The remote service has one of two configurations that are known to be required for the CRIME attack:

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

Solution: Disable compression and / or the SPDY service.

See Also: http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?e8c92220
https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS Temporal Score: 3.6

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

- SSL / TLS compression is enabled.

CVE: CVE-2012-4929, CVE-2012-4930

BID: 55704, 55707

Crossref: OSVDB #85926, OSVDB #85927

Vulnerability Publication Date: 2012/09/15

Plugin Publication Date: 2012/10/16

Plugin Modification Date: 2013/03/18

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: ssl_crime.nasl

Synopsis: The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description: The remote service has one of two configurations that are known to be required for the CRIME attack:

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

Solution: Disable compression and / or the SPDY service.

See Also: http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
https://discussions.nessus.org/thread/5546
http://www.nessus.org/u?e8c92220
https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.6

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

CPE:

CVE: CVE-2012-4929,CVE-2012-4930

BID: 55704,55707

Cross References: OSVDB #85926,OSVDB #85927

First Discovered: Feb 4, 2013 10:05:13 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Sep 15, 2012 12:00:00 EDT

Patch Publication Date: N/A

Plugin Publication Date: Oct 16, 2012 12:00:00 EDT

Plugin Modification Date: Mar 18, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.7

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.2

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.24

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-3499, CVE-2012-4558

BID: 58165

Crossref: OSVDB #90556, OSVDB #90557

Vulnerability Publication Date: 2013/02/18

Patch Publication Date: 2013/02/26

Plugin Publication Date: 2013/02/27

Plugin Modification Date: 2013/09/15

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_24.nasl

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.2

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-3499,CVE-2012-4558

BID: 58165

Cross References: OSVDB #90556,OSVDB #90557

First Discovered: Mar 4, 2013 10:04:55 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Feb 18, 2013 12:00:00 EST

Patch Publication Date: Feb 26, 2013 12:00:00 EST

Plugin Publication Date: Feb 27, 2013 12:00:00 EST

Plugin Modification Date: Sep 15, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.2

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.24
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-3499, CVE-2012-4558

BID: 58165

Crossref: OSVDB #90556, OSVDB #90557

Vulnerability Publication Date: 2013/02/18

Patch Publication Date: 2013/02/26

Plugin Publication Date: 2013/02/27

Plugin Modification Date: 2013/09/15

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_24.nasl

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3
CVSS Temporal Score: 3.2
CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C
CPE: cpe:/a:apache:http_server
CVE: CVE-2012-3499,CVE-2012-4558
BID: 58165
Cross References: OSVDB #90556,OSVDB #90557
First Discovered: Mar 4, 2013 10:04:55 EST
Last Observed: Nov 4, 2013 10:37:50 EST
Vuln Publication Date: Feb 18, 2013 12:00:00 EST
Patch Publication Date: Feb 26, 2013 12:00:00 EST
Plugin Publication Date: Feb 27, 2013 12:00:00 EST
Plugin Modification Date: Sep 15, 2013 12:00:00 EDT
Exploit Ease: No known exploits are available
Exploit Frameworks:
Check Type: remote
Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilit	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	No

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

CVSS Base Score: 4.3

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS Temporal Score: 3.2

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.24

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-3499, CVE-2012-4558

BID: 58165

Crossref: OSVDB #90556, OSVDB #90557

Vulnerability Publication Date: 2013/02/18

Patch Publication Date: 2013/02/26

Plugin Publication Date: 2013/02/27

Plugin Modification Date: 2013/09/15

Exploit Available: false

Exploitability Ease: No known exploits are available

Plugin Type: remote

Source File: apache_2_2_24.nasl

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

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

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.

See Also: http://www.apache.org/dist/httpd/CHANGES_2.2.24
http://httpd.apache.org/security/vulnerabilities_22.html

Risk Factor: Medium

STIG Severity:

CVSS Base Score: 4.3

CVSS Temporal Score: 3.2

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2012-3499,CVE-2012-4558

BID: 58165

Cross References: OSVDB #90556,OSVDB #90557

First Discovered: Mar 4, 2013 10:04:55 EST

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: Feb 18, 2013 12:00:00 EST

Patch Publication Date: Feb 26, 2013 12:00:00 EST

Plugin Publication Date: Feb 27, 2013 12:00:00 EST

Plugin Modification Date: Sep 15, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.8

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.25 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	80	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 4.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.25

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862, CVE-2013-1896

BID: 59826, 61129

Crossref: OSVDB #93366, OSVDB #95498, IAVA #2013-A-0146

Vulnerability Publication Date: 2013/05/13

Patch Publication Date: 2013/07/10

Plugin Publication Date: 2013/07/16

Plugin Modification Date: 2013/09/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_25.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Temporal Score: 4.2

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862,CVE-2013-1896

BID: 59826,61129

Cross References: OSVDB #93366,OSVDB #95498,IAVA #2013-A-0146

First Discovered: Aug 5, 2013 12:24:36 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 13, 2013 12:00:00 EDT

Patch Publication Date: Jul 10, 2013 12:00:00 EDT

Plugin Publication Date: Jul 16, 2013 12:00:00 EDT

Plugin Modification Date: Sep 15, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:	
Check Type: remote	
Version: Revision: 1.6	

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 < 2.2.25 Multiple Vulnerabilit	Medium	10.3.0.122	REP_CIT	443	TCP	Web Servers	Yes

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 4.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:

```
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.25
```

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862, CVE-2013-1896

BID: 59826, 61129

Crossref: OSVDB #93366, OSVDB #95498, IAVA #2013-A-0146

Vulnerability Publication Date: 2013/05/13

Patch Publication Date: 2013/07/10

Plugin Publication Date: 2013/07/16

Plugin Modification Date: 2013/09/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_25.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Temporal Score: 4.2

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862,CVE-2013-1896

BID: 59826,61129

Cross References: OSVDB #93366,OSVDB #95498,IAVA #2013-A-0146

First Discovered: Aug 5, 2013 12:24:36 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 13, 2013 12:00:00 EDT

Patch Publication Date: Jul 10, 2013 12:00:00 EDT

Plugin Publication Date: Jul 16, 2013 12:00:00 EDT

Plugin Modification Date: Sep 15, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.6

Plugin Name	Severity	IP Address	Repository	Port	Protocol	Family	Exploit?
Apache 2.2 <	Medium	10.3.0.122	REP_CIT	8457	TCP	Web Servers	Yes

2.2.25
Multiple
Vulnerabilit

MAC Address: 00:50:56:8b:1c:9d

DNS Name: telmaxdr.victrackad.victrack.com.au

NetBIOS Name: VICTRACKAD\TELMAX21

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSS Temporal Score: 4.2

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Plugin Output:
Version source : Server: Apache/2.2.6
Installed version : 2.2.6
Fixed version : 2.2.25

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862, CVE-2013-1896

BID: 59826, 61129

Crossref: OSVDB #93366, OSVDB #95498, IAVA #2013-A-0146

Vulnerability Publication Date: 2013/05/13

Patch Publication Date: 2013/07/10

Plugin Publication Date: 2013/07/16

Plugin Modification Date: 2013/09/15

Exploit Available: true

Exploitability Ease: Exploits are available

Plugin Type: remote

Source File: apache_2_2_25.nasl

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

Description: According to its banner, the version of Apache 2.2 installed on the remote host is earlier than 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

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

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

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

Solution: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.25 or later.

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

Risk Factor: Medium

STIG Severity: I

CVSS Base Score: 5.1

CVSS Temporal Score: 4.2

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

CPE: cpe:/a:apache:http_server

CVE: CVE-2013-1862,CVE-2013-1896

BID: 59826,61129

Cross References: OSVDB #93366,OSVDB #95498,IAVA #2013-A-0146

First Discovered: Aug 5, 2013 12:24:36 EDT

Last Observed: Nov 4, 2013 10:37:50 EST

Vuln Publication Date: May 13, 2013 12:00:00 EDT

Patch Publication Date: Jul 10, 2013 12:00:00 EDT

Plugin Publication Date: Jul 16, 2013 12:00:00 EDT

Plugin Modification Date: Sep 15, 2013 12:00:00 EDT

Exploit Ease: Exploits are available

Exploit Frameworks:

Check Type: remote

Version: Revision: 1.6