

Scan Report

September 7, 2014

Summary

This document reports on the results of an automatic security scan. The scan started at Sun Sep 7 02:14:15 2014 UTC and ended at Sun Sep 7 02:52:20 2014 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
2	Results per Host	2
2.1	192.168.56.101	2
2.1.1	High http (80/tcp)	2
2.1.2	High https (443/tcp)	5
2.1.3	High ssh (22/tcp)	9
2.1.4	Medium http (80/tcp)	10
2.1.5	Medium https (443/tcp)	14
2.1.6	Medium ssh (22/tcp)	19
2.1.7	Medium general/tcp	20
2.2	192.168.56.103	21
2.2.1	High http (80/tcp)	21
2.2.2	High https (443/tcp)	29
2.2.3	Medium http (80/tcp)	38
2.2.4	Medium https (443/tcp)	40
2.2.5	Medium general/tcp	42
2.2.6	Medium ssh (22/tcp)	42

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.56.101 (KIOPTRIX)	Severity: High	14	14	0	0	0
192.168.56.103	Severity: High	39	9	0	0	0
Total: 2		53	23	0	0	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level "Low" are not shown.

Issues with the threat level "Log" are not shown.

Issues with the threat level "Debug" are not shown.

Issues with the threat level "False Positive" are not shown.

This report contains all 76 results selected by the filtering described above. Before filtering there were 165 results.

2 Results per Host

2.1 192.168.56.101

Host scan start Sun Sep 7 02:14:22 2014 UTC

Host scan end Sun Sep 7 02:52:19 2014 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
ssh (22/tcp)	High
http (80/tcp)	Medium
https (443/tcp)	Medium
ssh (22/tcp)	Medium
general/tcp	Medium

2.1.1 High http (80/tcp)

High (CVSS: 10.0)

NVT: OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability

Summary:

OpenSSL is prone to an unspecified vulnerability in bn_wexpend().

...continues on next page ...

...continued from previous page ...
<p>According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8m which is vulnerable.</p> <p>Solution:</p> <p>The vendor has released updates. Please see the references for more information.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.100527</p>
<p>References</p> <p>CVE: CVE-2009-3245</p> <p>BID:38562</p> <p>Other:</p> <p>URL:http://www.securityfocus.com/bid/38562</p> <p>URL:http://openssl.org/</p>

High (CVSS: 7.5)

NVT: OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability

Summary:

OpenSSL is prone to a remote memory-corruption vulnerability. According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8o/1.0.0a which is vulnerable. An attacker can exploit this issue by supplying specially crafted structures to a vulnerable application that uses the affected library. Successfully exploiting this issue can allow the attacker to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition. Versions of OpenSSL 0.9.h through 0.9.8n and OpenSSL 1.0.x prior to 1.0.0a are affected. Note that Cryptographic Message Syntax (CMS) functionality is only enabled by default in OpenSSL versions 1.0.x.

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100668

References

CVE: CVE-2010-0742

BID:40502

Other:

URL:<https://www.securityfocus.com/bid/40502>

...continues on next page ...

...continued from previous page ...

URL:<http://www.openssl.org>

URL:http://www.openssl.org/news/secadv_20100601.txt

High (CVSS: 7.5)

NVT: Webalizer Cross Site Scripting Vulnerability

Summary:

Webalizer have a cross-site scripting vulnerability, that could allow malicious HTML tags to be injected in the reports generated by the Webalizer.

Solution:

Upgrade to Version 2.01-09 and change the directory in 'OutputDir'

OID of test routine: 1.3.6.1.4.1.25623.1.0.10816

References

CVE: CVE-2001-0835

BID:3473

High (CVSS: 7.5)

NVT: mod_ssl hook functions format string vulnerability

Summary:

The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.

*** Some vendors patched older versions of mod_ssl, so this
*** might be a false positive. Check with your vendor to determine
*** if you have a version of mod_ssl that is patched for this
*** vulnerability

Solution:

Upgrade to version 2.8.19 or newer

OID of test routine: 1.3.6.1.4.1.25623.1.0.13651

References

CVE: CVE-2004-0700

BID:10736

High (CVSS: 5.8)
NVT: http TRACE XSS attack

Summary:

Debugging functions are enabled on the remote HTTP server.

Description :

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

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

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

Solution:

Disable these methods.

Plugin output :

Solution:

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

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

See also <http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

OID of test routine: 1.3.6.1.4.1.25623.1.0.11213

References

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

BID:9506, 9561, 11604

Other:

URL:<http://www.kb.cert.org/vuls/id/867593>

[\[return to 192.168.56.101 \]](#)

2.1.2 High https (443/tcp)

High (CVSS: 10.0)
NVT: OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability

Summary:

OpenSSL is prone to an unspecified vulnerability in bn_wexpend(). According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8m which is vulnerable.

Solution:

The vendor has released updates. Please see the references for more

...continues on next page ...

...continued from previous page ...

information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100527

References

CVE: CVE-2009-3245

BID:38562

Other:

URL:<http://www.securityfocus.com/bid/38562>URL:<http://openssl.org/>**High (CVSS: 7.5)****NVT: OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability****Summary:**

OpenSSL is prone to a remote memory-corruption vulnerability. According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8o/1.0.0a which is vulnerable

An attacker can exploit this issue by supplying specially crafted structures to a vulnerable application that uses the affected library. Successfully exploiting this issue can allow the attacker to execute arbitrary code. Failed exploit attempts will result in a denial-of-service condition.

Versions of OpenSSL 0.9.h through 0.9.8n and OpenSSL 1.0.x prior to 1.0.0a are affected. Note that Cryptographic Message Syntax (CMS) functionality is only enabled by default in OpenSSL versions 1.0.x.

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100668

References

CVE: CVE-2010-0742

BID:40502

Other:

URL:<https://www.securityfocus.com/bid/40502>URL:<http://www.openssl.org>URL:http://www.openssl.org/news/secadv_20100601.txt

High (CVSS: 7.5)
NVT: Webalizer Cross Site Scripting Vulnerability**Summary:**

Webalizer have a cross-site scripting vulnerability, that could allow malicious HTML tags to be injected in the reports generated by the Webalizer.

Solution:

Upgrade to Version 2.01-09 and change the directory in 'OutputDir'

OID of test routine: 1.3.6.1.4.1.25623.1.0.10816

References

CVE: CVE-2001-0835

BID:3473

High (CVSS: 7.5)
NVT: HTTP Windows 98 MS/DOS device names DOS

It was possible to kill your web server by reading a MS/DOS device, using a file name like CON\CON, AUX.htm or AUX.

A cracker may use this flaw to make your server crash continuously, preventing you from working properly.

Solution: upgrade your system or use a HTTP server that filters those names out.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10930

References

CVE: CVE-2001-0386, CVE-2001-0493, CVE-2001-0391, CVE-2001-0558, CVE-2002-0200, ↪ CVE-2000-0168, CVE-2003-0016, CVE-2001-0602

BID:1043, 2575, 2608, 2622, 2649, 2704, 3929, 6659, 6662

Other:

IAVA:2003-t-0003

High (CVSS: 7.5)
NVT: mod_ssl hook functions format string vulnerability**Summary:**

... continues on next page ...

...continued from previous page ...
<p>The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.</p> <p>*** Some vendors patched older versions of mod_ssl, so this *** might be a false positive. Check with your vendor to determine *** if you have a version of mod_ssl that is patched for this *** vulnerability</p> <p>Solution: Upgrade to version 2.8.19 or newer</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.13651</p>
<p>References CVE: CVE-2004-0700 BID:10736</p>

<p>High (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability</p>
<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.105042</p>
<p>References CVE: CVE-2014-0224 BID:67899 Other: URL:http://www.securityfocus.com/bid/67899 URL:http://openssl.org/</p>

<p>High (CVSS: 5.8) NVT: http TRACE XSS attack</p>
<p>Summary: Debugging functions are enabled on the remote HTTP server.</p> <p>Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to</p>
...continues on next page ...

<p>...continued from previous page ...</p> <p>cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution:</p> <p>Disable these methods.</p> <p>Plugin output :</p> <p>Solution:</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.11213</p>
<p>References</p> <p>CVE: CVE-2004-2320, CVE-2003-1567</p> <p>BID:9506, 9561, 11604</p> <p>Other:</p> <p>URL:http://www.kb.cert.org/vuls/id/867593</p>

[\[return to 192.168.56.101 \]](#)

2.1.3 High ssh (22/tcp)

<p>High (CVSS: 10.0)</p> <p>NVT: OpenSSH 'sshd' Challenge Response Authentication Buffer Overflow Vulnerability</p>
<p>Summary:</p> <p>The host is running OpenSSH sshd with ChallengeResponseAuthentication enabled and is prone to buffer overflow vulnerability.</p> <p>Vulnerability Insight:</p> <p>The flaw is due to an error in handling a large number of responses during challenge response authentication when using PAM modules with interactive keyboard authentication (PAMAuthenticationViaKbdInt).</p> <p>Impact:</p> <p>Successful exploitation could allows remote attackers to execute arbitrary code and gain escalated privileges.</p> <p>Impact Level: Application</p> <p>Affected Software/OS:</p> <p>OpenSSH versions 2.3.1 to 3.3</p> <p>Solution:</p>
<p>...continues on next page ...</p>

...continued from previous page ...
Upgrade to OpenSSH version 3.4 or later For updates refer to http://www.openssh.com/
OID of test routine: 1.3.6.1.4.1.25623.1.0.802407
References CVE: CVE-2002-0640 BID:5093 Other: URL: http://osvdb.org/839 URL: http://www.kb.cert.org/vuls/id/369347 URL: http://www.cert.org/advisories/CA-2002-18.html URL: http://marc.info/?l=bugtraq&m=102521542826833&w=2

High (CVSS: 7.5)

NVT: OpenSSH AFS/Kerberos ticket/token passing

Summary:

You are running a version of OpenSSH older than OpenSSH 3.2.1
A buffer overflow exists in the daemon if AFS is enabled on
your system, or if the options KerberosTgtPassing or
AFSTokenPassing are enabled. Even in this scenario, the
vulnerability may be avoided by enabling UsePrivilegeSeparation.
Versions prior to 2.9.9 are vulnerable to a remote root
exploit. Versions prior to 3.2.1 are vulnerable to a local
root exploit.

Solution:

Upgrade to the latest version of OpenSSH

OID of test routine: 1.3.6.1.4.1.25623.1.0.10954

References

CVE: CVE-2002-0575

BID:4560

[[return to 192.168.56.101](#)]

2.1.4 Medium http (80/tcp)

Medium (CVSS: 5.0)

NVT: OpenSSL 'ssl3_get_record()' Remote Denial of Service Vulnerability

Summary:

OpenSSL is prone to a denial-of-service vulnerability caused by a NULL-pointer dereference.
According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8n which is vulnerable. An attacker can exploit this issue to crash the affected application, denying service to legitimate users.
OpenSSL versions 0.9.8f through 0.9.8m are vulnerable.

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100587

References

CVE: CVE-2010-0740

BID:39013

Other:

URL:<http://www.securityfocus.com/bid/39013>

URL:<http://www.openbsd.org/errata45.html>

URL:<http://www.openbsd.org/errata46.html>

URL:<http://www.openbsd.org/errata47.html>

URL:<http://www.openssl.org>

URL:<http://www.securityfocus.com/archive/1/510726>

URL:http://openssl.org/news/secadv_20100324.txt

Medium (CVSS: 5.0)

NVT: Apache UserDir Sensitive Information Disclosure

Summary:

An information leak occurs on Apache based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

Solution:

1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.:

RedirectMatch ^/~(.*)\$ http://my-target-webserver.somewhere.org/\$1

Or

...continues on next page ...

...continued from previous page ...

3) Add into httpd.conf:
 ErrorDocument 404 http://localhost/sample.html
 ErrorDocument 403 http://localhost/sample.html
 (NOTE: You need to use a FQDN inside the URL for it to work properly).
 Additional Information:
<http://www.securiteam.com/unixfocus/5WPOC1F5FI.html>

OID of test routine: 1.3.6.1.4.1.25623.1.0.10766

References

CVE: CVE-2001-1013
 BID:3335

Medium (CVSS: 4.3)

NVT: OpenSSL 'dtls1_retrieve_buffered_fragment()' Remote Denial of Service Vulnerability

Summary:

OpenSSL is prone to a denial-of-service vulnerability caused by a NULL-pointer dereference.
 According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8n which is vulnerable.
 An attacker can exploit this issue to crash the affected application, denying service to legitimate users.
 OpenSSL versions 0.9.8m and prior are vulnerable.

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100588

References

CVE: CVE-2010-0433
 BID:38533

Other:

URL:<http://www.securityfocus.com/bid/38533>
 URL:https://bugzilla.redhat.com/show_bug.cgi?id=567711
 URL:https://bugzilla.redhat.com/show_bug.cgi?id=569774
 URL:<http://www.openwall.com/lists/oss-security/2010/03/03/5>
 URL:<http://cvs.openssl.org/chngview?cn=19374>
 URL:<http://www.openssl.org>
 URL:<http://www.securityfocus.com/archive/1/510726>

Medium (CVSS: 4.3)**NVT: Apache Web Server ETag Header Information Disclosure Weakness****Summary:**

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network. OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Solution:

OpenBSD has released a patch to address this issue.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Information that was gathered:

Inode: 34821

Size: 2890

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

CVE: CVE-2003-1418

BID:6939

Other:

URL:<https://www.securityfocus.com/bid/6939>

URL:<http://httpd.apache.org/docs/mod/core.html#fileetag>

URL:<http://www.openbsd.org/errata32.html>

URL:<http://support.novell.com/docs/Tids/Solutions/10090670.html>

Medium (CVSS: 4.3)**NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability****Summary:**

This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Insight:

The flaw is due to an error within the default error response for

... continues on next page ...

<p>...continued from previous page ...</p> <p>status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.</p> <p>Impact: Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.</p> <p>Impact Level: Application</p> <p>Affected Software/OS: Apache HTTP Server versions 2.2.0 through 2.2.21</p> <p>Solution: Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.902830</p>
<p>References</p> <p>CVE: CVE-2012-0053</p> <p>BID:51706</p> <p>Other:</p> <p>URL:http://osvdb.org/78556</p> <p>URL:http://secunia.com/advisories/47779</p> <p>URL:http://www.exploit-db.com/exploits/18442</p> <p>URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html</p> <p>URL:http://httpd.apache.org/security/vulnerabilities_22.html</p> <p>URL:http://svn.apache.org/viewvc?view=revision&revision=1235454</p> <p>URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm</p> <p>↪1</p>

[[return to 192.168.56.101](#)]

2.1.5 Medium https (443/tcp)

<p>Medium (CVSS: 5.0)</p> <p>NVT: OpenSSL 'ssl3_get_record()' Remote Denial of Service Vulnerability</p>
<p>Summary:</p> <p>OpenSSL is prone to a denial-of-service vulnerability caused by a NULL-pointer dereference.</p> <p>According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8n which is vulnerable. An attacker can exploit this issue to crash the affected application, denying service to legitimate users.</p> <p>OpenSSL versions 0.9.8f through 0.9.8m are vulnerable.</p> <p>Solution:</p>
<p>...continues on next page ...</p>

...continued from previous page ...

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100587

References

CVE: CVE-2010-0740

BID:39013

Other:

URL:<http://www.securityfocus.com/bid/39013>

URL:<http://www.openbsd.org/errata45.html>

URL:<http://www.openbsd.org/errata46.html>

URL:<http://www.openbsd.org/errata47.html>

URL:<http://www.openssl.org>

URL:<http://www.securityfocus.com/archive/1/510726>

URL:http://openssl.org/news/secadv_20100324.txt

Medium (CVSS: 5.0)

NVT: Apache UserDir Sensitive Information Disclosure

Summary:

An information leak occurs on Apache based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

Solution:

1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.:

RedirectMatch ^/~(.*)\$ http://my-target-webserver.somewhere.org/\$1

Or

3) Add into httpd.conf:

ErrorDocument 404 http://localhost/sample.html

ErrorDocument 403 http://localhost/sample.html

(NOTE: You need to use a FQDN inside the URL for it to work properly).

Additional Information:

<http://www.securiteam.com/unixfocus/5WPOC1F5FI.html>

OID of test routine: 1.3.6.1.4.1.25623.1.0.10766

...continues on next page ...

...continued from previous page ...

References

CVE: CVE-2001-1013

BID:3335

Medium (CVSS: 4.3)

NVT: OpenSSL 'dtls1_retrieve_buffered_fragment()' Remote Denial of Service Vulnerability

Summary:

OpenSSL is prone to a denial-of-service vulnerability caused by a NULL-pointer dereference. According to its banner, OpenVAS has discovered that the remote Webserver is using a version prior to OpenSSL 0.9.8n which is vulnerable. An attacker can exploit this issue to crash the affected application, denying service to legitimate users. OpenSSL versions 0.9.8m and prior are vulnerable.

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.100588

References

CVE: CVE-2010-0433

BID:38533

Other:

URL:<http://www.securityfocus.com/bid/38533>
URL:https://bugzilla.redhat.com/show_bug.cgi?id=567711
URL:https://bugzilla.redhat.com/show_bug.cgi?id=569774
URL:<http://www.openwall.com/lists/oss-security/2010/03/03/5>
URL:<http://cvs.openssl.org/chngview?cn=19374>
URL:<http://www.openssl.org>
URL:<http://www.securityfocus.com/archive/1/510726>

Medium (CVSS: 4.3)

NVT: Apache Web Server ETag Header Information Disclosure Weakness

Summary:

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the

...continues on next page ...

...continued from previous page ...

file's inode number.

Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network. OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

Solution:

OpenBSD has released a patch to address this issue.

Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Information that was gathered:

Inode: 34821

Size: 2890

OID of test routine: 1.3.6.1.4.1.25623.1.0.103122

References

CVE: CVE-2003-1418

BID:6939

Other:

URL:<https://www.securityfocus.com/bid/6939>

URL:<http://httpd.apache.org/docs/mod/core.html#fileetag>

URL:<http://www.openbsd.org/errata32.html>

URL:<http://support.novell.com/docs/Tids/Solutions/10090670.html>

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers

Summary:

This routine search for weak SSL ciphers offered by a service.

Vulnerability Insight:

These rules are applied for the evaluation of the cryptographic strength:

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky

...continues on next page ...

...continued from previous page ...

↔ 13 attacks

- Any cipher considered to be secure for only the next 10 years is considered as

↔ medium

- Any other cipher is considered as strong

Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Weak ciphers offered by this service:

```

SSL2_RC4_128_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC2_CBC_128_CBC_WITH_MD5
SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
SSL3_RSA_RC4_40_MD5
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
SSL3_RSA_RC2_40_MD5
SSL3_RSA_DES_40_CBC_SHA
SSL3_RSA_DES_64_CBC_SHA
SSL3_EDH_RSA_DES_40_CBC_SHA
SSL3_EDH_RSA_DES_64_CBC_SHA
SSL3_RSA_EXPORT1024_WITH_RC4_56_MD5, weak authentication
SSL3_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5, weak authentication
SSL3_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
SSL3_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication
TLS1_RSA_RC4_40_MD5
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC2_40_MD5
TLS1_RSA_DES_40_CBC_SHA
TLS1_RSA_DES_64_CBC_SHA
TLS1_EDH_RSA_DES_40_CBC_SHA
TLS1_EDH_RSA_DES_64_CBC_SHA
TLS1_RSA_EXPORT1024_WITH_RC4_56_MD5, weak authentication
TLS1_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5, weak authentication
TLS1_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
TLS1_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication

```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary:

This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

...continues on next page ...

...continued from previous page ...

Vulnerability Insight:

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Impact:

Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Impact Level: Application

Affected Software/OS:

Apache HTTP Server versions 2.2.0 through 2.2.21

Solution:

Upgrade to Apache HTTP Server version 2.2.22 or later,
For updates refer to <http://httpd.apache.org/>

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

References

CVE: CVE-2012-0053

BID:51706

Other:

URL:<http://osvdb.org/78556>

URL:<http://secunia.com/advisories/47779>

URL:<http://www.exploit-db.com/exploits/18442>

URL:<http://rhn.redhat.com/errata/RHSA-2012-0128.html>

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

URL:<http://svn.apache.org/viewvc?view=revision&revision=1235454>

URL:<http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm>

↪1

Medium (CVSS: 0.0)

NVT: SSL Certificate Expiry

The SSL certificate of the remote service expired on 2010-09-26 09:32:06 UTC!

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[\[return to 192.168.56.101 \]](#)

2.1.6 Medium ssh (22/tcp)

Medium (CVSS: 3.5) NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability
<p>According to its banner, the version of OpenSSH installed on the remote host is older than 5.7:</p> <pre>ssh-1.99-openssh_2.9p2</pre> <p>Summary:</p> <p>The <code>auth_parse_options</code> function in <code>auth-options.c</code> in <code>sshd</code> in OpenSSH before 5.7 provides debug messages containing <code>authorized_keys</code> command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an <code>authorized_keys</code> file in its own home directory. OpenSSH before 5.7 is affected;</p> <p>Solution:</p> <p>Updates are available. Please see the references for more information.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.103503</p>
<p>References</p> <p>CVE: CVE-2012-0814</p> <p>BID:51702</p> <p>Other:</p> <p>URL:http://www.securityfocus.com/bid/51702</p> <p>URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445</p> <p>URL:http://packages.debian.org/squeeze/openssh-server</p> <p>URL:https://downloads.avaya.com/css/P8/documents/100161262</p>

[[return to 192.168.56.101](#)]

2.1.7 Medium general/tcp

Medium (CVSS: 2.6) NVT: TCP timestamps
<p>It was detected that the host implements RFC1323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Paket 1: 15643684</p> <p>Paket 2: 15643815</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.80091</p> <p>...continues on next page ...</p>

...continued from previous page ...

References

Other:

URL:<http://www.ietf.org/rfc/rfc1323.txt>[\[return to 192.168.56.101 \]](#)**2.2 192.168.56.103**

Host scan start Sun Sep 7 02:14:22 2014 UTC

Host scan end Sun Sep 7 02:43:00 2014 UTC

Service (Port)	Threat Level
http (80/tcp)	High
https (443/tcp)	High
http (80/tcp)	Medium
https (443/tcp)	Medium
general/tcp	Medium
ssh (22/tcp)	Medium

2.2.1 High http (80/tcp)

High (CVSS: 10.0)

NVT: PHP version smaller than 5.2.7

Summary:

PHP version smaller than 5.2.7 suffers vulnerability.

Solution:

Update PHP to version 5.2.7 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110172

References

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

High (CVSS: 10.0) NVT: PHP version smaller than 5.2.0
<p>Summary: PHP version smaller than 5.2.0 suffers vulnerability.</p> <p>Solution: Update PHP to version 5.2.0 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110173</p>
<p>References CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625, ↪ CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE ↪ -2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424 BID: 20349, 20879, 49634</p>

High (CVSS: 10.0) NVT: PHP version smaller than 4.4.5
<p>Summary: PHP version smaller than 4.4.5 suffers vulnerability.</p> <p>Solution: Update PHP to version 4.4.5 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110174</p>
<p>References CVE: CVE-2006-4625, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, ↪ CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1286, CVE-2007-1376, CVE ↪ -2007-1378, CVE-2007-1379, CVE-2007-1380, CVE-2007-1700, CVE-2007-1701, CVE-20 ↪ 07-1777, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007- ↪ 1886, CVE-2007-1887, CVE-2007-1890 BID: 22496, 22805, 22806, 22833, 22862, 23119, 23120, 23169, 23219, 23233, 23234, ↪ 23235, 23236</p>

High (CVSS: 10.0) NVT: PHP version smaller than 5.2.1
<p>Summary: PHP version smaller than 5.2.1 suffers vulnerability.</p>
...continues on next page ...

<p>...continued from previous page ...</p> <p>Solution: Update PHP to version 5.2.1 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110175</p>
<p>References CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908, ↪ CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE- ↪ 2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-20 ↪ 07-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007- ↪ 1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-444 ↪ 1, CVE-2007-4586 BID: 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234, ↪ 23235, 23236, 23237, 23238</p>

High (CVSS: 10.0)
 NVT: PHP version smaller than 5.2.6

Summary:
 PHP version smaller than 5.2.6 suffers vulnerability.
Solution:
 Update PHP to version 5.2.6 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110183

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

High (CVSS: 9.3)
 NVT: PHP version smaller than 5.2.14

Summary:
 PHP version smaller than 5.2.14 suffers vulnerability.
Solution:
 Update PHP to version 5.2.14 or later.

...continues on next page ...

...continued from previous page ...
OID of test routine: 1.3.6.1.4.1.25623.1.0.110171
References 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

High (CVSS: 9.3) NVT: PHP version smaller than 5.1.2
Summary: PHP version smaller than 5.1.2 suffers vulnerability. Solution: Update PHP to version 5.1.2 or later. OID of test routine: 1.3.6.1.4.1.25623.1.0.110177
References CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208 BID:16220, 16803

High (CVSS: 9.3) NVT: PHP version smaller than 5.2.5
Summary: PHP version smaller than 5.2.5 suffers vulnerability. Solution: Update PHP to version 5.2.5 or later. OID of test routine: 1.3.6.1.4.1.25623.1.0.110179
References CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825, ↔CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE ↔-2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20 ↔08-4107
...continues on next page ...

...continued from previous page ...

BID:26403

High (CVSS: 9.3)

NVT: PHP version smaller than 5.3.3

Summary:

PHP version smaller than 5.3.3 suffers vulnerability.

Solution:

Update PHP to version 5.3.3 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110182

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
↔CVE-2010-1917, 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-2010-3062, CVE-20
↔10-3063, CVE-2010-3064, CVE-2010-3065
BID:38708, 40461, 40948, 41991

High (CVSS: 9.3)

NVT: PHP version smaller than 4.4.4

Summary:

PHP version smaller than 4.4.4 suffers vulnerability.

Solution:

Update PHP to version 4.4.4 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110188

References

CVE: CVE-2006-1017, CVE-2006-4020
BID:16878, 19415

High (CVSS: 7.8)

NVT: PHP version smaller than 5.2.2

Summary:

PHP version smaller than 5.2.2 suffers vulnerability.

...continues on next page ...

<p>...continued from previous page ...</p> <p>Solution: Update PHP to version 5.2.2 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110185</p>
<p>References CVE: CVE-2007-1649 BID:23105</p>

<p>High (CVSS: 7.5) NVT: PHP version smaller than 5.2.11</p>
<p>Summary: PHP version smaller than 5.2.11 suffers vulnerability. Solution: Update PHP to version 5.2.11 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110176</p>
<p>References CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, ↔CVE-2009-5016 BID:36449, 44889</p>

<p>High (CVSS: 7.5) NVT: PHP version smaller than 5.3.1</p>
<p>Summary: PHP version smaller than 5.3.1 suffers vulnerability. Solution: Update PHP to version 5.3.1 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110178</p>
<p>References CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128 ...continues on next page ...</p>

...continued from previous page ...

BID:36554, 36555, 37079, 37138

<p>High (CVSS: 7.5)</p>

<p>NVT: PHP version smaller than 5.2.8</p>

<p>Summary:</p>

<p>PHP version smaller than 5.2.8 suffers vulnerability.</p>

<p>Solution:</p>

<p>Update PHP to version 5.2.8 or later.</p>

<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110180</p>

<p>References</p>

<p>CVE: CVE-2008-5814, CVE-2008-5844</p>

<p>BID:32673</p>

<p>High (CVSS: 7.5)</p>

<p>NVT: PHP version smaller than 5.2.4</p>

<p>Summary:</p>

<p>PHP version smaller than 5.2.4 suffers vulnerability.</p>

<p>Solution:</p>

<p>Update PHP to version 5.2.4 or later.</p>

<p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110184</p>

<p>References</p>

<p>CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790, ↪ CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE ↪ -2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-20 ↪ 07-4661, CVE-2007-4662, CVE-2007-4663</p>

<p>BID:24661, 24261, 24922, 25498</p>

<p>High (CVSS: 7.5)</p>

<p>NVT: PHP version smaller than 4.4.8</p>

<p>Summary:</p>

<p>PHP version smaller than 4.4.8 suffers vulnerability.</p>

<p>...continues on next page ...</p>

<p>...continued from previous page ...</p> <p>Solution: Update PHP to version 4.4.8 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110186</p>
<p>References CVE: CVE-2007-3378, CVE-2007-3997, CVE-2007-3799, CVE-2007-4657, CVE-2007-4658, ↪ CVE-2008-0145, CVE-2008-2108 BID: 24661, 49631</p>

<p>High (CVSS: 6.8) NVT: PHP version smaller than 5.3.4</p>
<p>Summary: PHP version smaller than 5.3.4 suffers vulnerability. Solution: Update PHP to version 5.3.4 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110181</p>
<p>References CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709, ↪ CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE ↪ -2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20 ↪ 11-0754, CVE-2011-0755 BID: 40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339, ↪ 45952, 45954, 46056, 46168</p>

<p>High (CVSS: 6.8) NVT: PHP version smaller than 5.2.3</p>
<p>Summary: PHP version smaller than 5.2.3 suffers vulnerability. Solution: Update PHP to version 5.2.3 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110189</p>
<p>...continues on next page ...</p>

...continued from previous page ...

References

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

High (CVSS: 5.8)**NVT: http TRACE XSS attack****Summary:**

Debugging functions are enabled on the remote HTTP server.

Description :

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

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

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

Solution:

Disable these methods.

Plugin output :**Solution:**

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

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

See also <http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

OID of test routine: 1.3.6.1.4.1.25623.1.0.11213

References

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

BID:9506, 9561, 11604

Other:

URL:<http://www.kb.cert.org/vuls/id/867593>

[\[return to 192.168.56.103 \]](#)

2.2.2 High https (443/tcp)

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.7

Summary:
PHP version smaller than 5.2.7 suffers vulnerability.
Solution:
Update PHP to version 5.2.7 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110172

References

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

High (CVSS: 10.0)
NVT: PHP version smaller than 5.2.0

Summary:
PHP version smaller than 5.2.0 suffers vulnerability.
Solution:
Update PHP to version 5.2.0 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110173

References

CVE: CVE-2006-1015, CVE-2006-1549, CVE-2006-2660, CVE-2006-4486, CVE-2006-4625,
↔CVE-2006-4812, CVE-2006-5465, CVE-2006-5706, CVE-2006-7205, CVE-2007-0448, CVE
↔-2007-1381, CVE-2007-1584, CVE-2007-1888, CVE-2007-2844, CVE-2007-5424
BID:20349, 20879, 49634

High (CVSS: 10.0)
NVT: PHP version smaller than 4.4.5

Summary:
PHP version smaller than 4.4.5 suffers vulnerability.
Solution:
Update PHP to version 4.4.5 or later.

...continues on next page ...

...continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.110174

References

CVE: CVE-2006-4625, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908,
 ↪ CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1286, CVE-2007-1376, CVE
 ↪ -2007-1378, CVE-2007-1379, CVE-2007-1380, CVE-2007-1700, CVE-2007-1701, CVE-20
 ↪ 07-1777, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-
 ↪ 1886, CVE-2007-1887, CVE-2007-1890
 BID: 22496, 22805, 22806, 22833, 22862, 23119, 23120, 23169, 23219, 23233, 23234,
 ↪ 23235, 23236

High (CVSS: 10.0)

NVT: PHP version smaller than 5.2.1

Summary:

PHP version smaller than 5.2.1 suffers vulnerability.

Solution:

Update PHP to version 5.2.1 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110175

References

CVE: CVE-2006-6383, CVE-2007-0905, CVE-2007-0906, CVE-2007-0907, CVE-2007-0908,
 ↪ CVE-2007-0909, CVE-2007-0910, CVE-2007-0988, CVE-2007-1376, CVE-2007-1380, CVE
 ↪ -2007-1383, CVE-2007-1452, CVE-2007-1453, CVE-2007-1454, CVE-2007-1700, CVE-20
 ↪ 07-1701, CVE-2007-1824, CVE-2007-1825, CVE-2007-1835, CVE-2007-1884, CVE-2007-
 ↪ 1885, CVE-2007-1886, CVE-2007-1887, CVE-2007-1889, CVE-2007-1890, CVE-2007-444
 ↪ 1, CVE-2007-4586
 BID: 21508, 22496, 22805, 22806, 22862, 22922, 23119, 23120, 23219, 23233, 23234,
 ↪ 23235, 23236, 23237, 23238

High (CVSS: 10.0)

NVT: PHP version smaller than 5.2.6

Summary:

PHP version smaller than 5.2.6 suffers vulnerability.

Solution:

Update PHP to version 5.2.6 or later.

...continues on next page ...

...continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.110183

References

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

BID:27413, 28392, 29009

High (CVSS: 9.3)

NVT: PHP version smaller than 5.2.14

Summary:

PHP version smaller than 5.2.14 suffers vulnerability.

Solution:

Update PHP to version 5.2.14 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110171

References

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

High (CVSS: 9.3)

NVT: PHP version smaller than 5.1.2

Summary:

PHP version smaller than 5.1.2 suffers vulnerability.

Solution:

Update PHP to version 5.1.2 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110177

References

CVE: CVE-2006-0200, CVE-2006-0207, CVE-2006-0208

BID:16220, 16803

High (CVSS: 9.3)

NVT: PHP version smaller than 5.2.5

Summary:

PHP version smaller than 5.2.5 suffers vulnerability.

Solution:

Update PHP to version 5.2.5 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110179

References

CVE: CVE-2007-3996, CVE-2007-4782, CVE-2007-4783, CVE-2007-4784, CVE-2007-4825,
 ↪ CVE-2007-4840, CVE-2007-4887, CVE-2007-4889, CVE-2007-5447, CVE-2007-5653, CVE
 ↪ -2007-5898, CVE-2007-5899, CVE-2007-5900, CVE-2008-2107, CVE-2008-2108, CVE-20
 ↪ 08-4107

BID:26403

High (CVSS: 9.3)

NVT: PHP version smaller than 5.3.3

Summary:

PHP version smaller than 5.3.3 suffers vulnerability.

Solution:

Update PHP to version 5.3.3 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110182

References

CVE: CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,
 ↪ CVE-2010-1917, 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-2010-3062, CVE-20
 ↪ 10-3063, CVE-2010-3064, CVE-2010-3065

BID:38708, 40461, 40948, 41991

High (CVSS: 9.3)

NVT: PHP version smaller than 4.4.4

Summary:

PHP version smaller than 4.4.4 suffers vulnerability.

Solution:

...continues on next page ...

...continued from previous page ...
Update PHP to version 4.4.4 or later.
OID of test routine: 1.3.6.1.4.1.25623.1.0.110188
References CVE: CVE-2006-1017, CVE-2006-4020 BID:16878, 19415

High (CVSS: 7.8) NVT: PHP version smaller than 5.2.2
Summary: PHP version smaller than 5.2.2 suffers vulnerability. Solution: Update PHP to version 5.2.2 or later.
OID of test routine: 1.3.6.1.4.1.25623.1.0.110185
References CVE: CVE-2007-1649 BID:23105

High (CVSS: 7.5) NVT: PHP version smaller than 5.2.11
Summary: PHP version smaller than 5.2.11 suffers vulnerability. Solution: Update PHP to version 5.2.11 or later.
OID of test routine: 1.3.6.1.4.1.25623.1.0.110176
References CVE: CVE-2009-3291, CVE-2009-3292, CVE-2009-3293, CVE-2009-3294, CVE-2009-4018, ↪CVE-2009-5016 BID:36449, 44889

High (CVSS: 7.5)

NVT: PHP version smaller than 5.3.1

Summary:

PHP version smaller than 5.3.1 suffers vulnerability.

Solution:

Update PHP to version 5.3.1 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110178

References

CVE: CVE-2009-3557, CVE-2009-3559, CVE-2009-4017, CVE-2009-4018, CVE-2010-1128
BID:36554, 36555, 37079, 37138

High (CVSS: 7.5)

NVT: PHP version smaller than 5.2.8

Summary:

PHP version smaller than 5.2.8 suffers vulnerability.

Solution:

Update PHP to version 5.2.8 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110180

References

CVE: CVE-2008-5814, CVE-2008-5844
BID:32673

High (CVSS: 7.5)

NVT: PHP version smaller than 5.2.4

Summary:

PHP version smaller than 5.2.4 suffers vulnerability.

Solution:

Update PHP to version 5.2.4 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110184

... continues on next page ...

...continued from previous page ...

References

CVE: CVE-2007-1413, CVE-2007-2872, CVE-2007-3294, CVE-2007-3378, CVE-2007-3790,
 ↪CVE-2007-3799, CVE-2007-3806, CVE-2007-4010, CVE-2007-4033, CVE-2007-4255, CVE
 ↪-2007-4507, CVE-2007-4652, CVE-2007-4658, CVE-2007-4659, CVE-2007-4660, CVE-20
 ↪07-4661, CVE-2007-4662, CVE-2007-4663
 BID:24661, 24261, 24922, 25498

High (CVSS: 7.5)

NVT: PHP version smaller than 4.4.8

Summary:

PHP version smaller than 4.4.8 suffers vulnerability.

Solution:

Update PHP to version 4.4.8 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110186

References

CVE: CVE-2007-3378, CVE-2007-3997, CVE-2007-3799, CVE-2007-4657, CVE-2007-4658,
 ↪CVE-2008-0145, CVE-2008-2108
 BID:24661, 49631

High (CVSS: 6.8)

NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID of test routine: 1.3.6.1.4.1.25623.1.0.105042

References

CVE: CVE-2014-0224

BID:67899

Other:

URL:<http://www.securityfocus.com/bid/67899>

URL:<http://openssl.org/>

...continues on next page ...

...continued from previous page ...

High (CVSS: 6.8)**NVT: PHP version smaller than 5.3.4****Summary:**

PHP version smaller than 5.3.4 suffers vulnerability.

Solution:

Update PHP to version 5.3.4 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110181

References

CVE: CVE-2006-7243, CVE-2010-2094, CVE-2010-2950, CVE-2010-3436, CVE-2010-3709,
 ↪ CVE-2010-3710, CVE-2010-3870, CVE-2010-4150, CVE-2010-4156, CVE-2010-4409, CVE
 ↪ -2010-4697, CVE-2010-4698, CVE-2010-4699, CVE-2010-4700, CVE-2011-0753, CVE-20
 ↪ 11-0754, CVE-2011-0755

BID: 40173, 43926, 44605, 44718, 44723, 44951, 44980, 45119, 45335, 45338, 45339,
 ↪ 45952, 45954, 46056, 46168

High (CVSS: 6.8)**NVT: PHP version smaller than 5.2.3****Summary:**

PHP version smaller than 5.2.3 suffers vulnerability.

Solution:

Update PHP to version 5.2.3 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110189

References

CVE: CVE-2007-1900, CVE-2007-2756, CVE-2007-2872, CVE-2007-3007

BID: 23359, 24089, 24259, 24261

High (CVSS: 5.8)**NVT: http TRACE XSS attack****Summary:**

Debugging functions are enabled on the remote HTTP server.

Description :

...continues on next page ...

<p>...continued from previous page ...</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p> <p>Solution:</p> <p>Disable these methods.</p> <p>Plugin output :</p> <p>Solution:</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.11213</p>
<p>References</p> <p>CVE: CVE-2004-2320, CVE-2003-1567</p> <p>BID:9506, 9561, 11604</p> <p>Other:</p> <p>URL:http://www.kb.cert.org/vuls/id/867593</p>

[[return to 192.168.56.103](#)]

2.2.3 Medium http (80/tcp)

<p>Medium (CVSS: 5.0)</p> <p>NVT: PHP version smaller than 5.1.0</p>
<p>Summary:</p> <p>PHP version smaller than 5.1.0 suffers vulnerability.</p> <p>Solution:</p> <p>Update PHP to version 5.1.0 or later.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.110170</p>
<p>References</p> <p>... continues on next page ...</p>

...continued from previous page ...

CVE: CVE-2005-3319, CVE-2005-3883
BID:15177, 15571

Medium (CVSS: 5.0)
NVT: PHP version smaller than 5.2.9

Summary:
PHP version smaller than 5.2.9 suffers vulnerability.
Solution:
Update PHP to version 5.2.9 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110187

References

CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
BID:33002, 33927

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary:
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.
Vulnerability Insight:
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.
Impact:
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application
Affected Software/OS:
Apache HTTP Server versions 2.2.0 through 2.2.21
Solution:
Upgrade to Apache HTTP Server version 2.2.22 or later,
For updates refer to <http://httpd.apache.org/>

OID of test routine: 1.3.6.1.4.1.25623.1.0.902830

...continues on next page ...

...continued from previous page ...

References

CVE: CVE-2012-0053

BID:51706

Other:

URL:http://osvdb.org/78556

URL:http://secunia.com/advisories/47779

URL:http://www.exploit-db.com/exploits/18442

URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html

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

URL:http://svn.apache.org/viewvc?view=revision&revision=1235454

URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm

↪1

[\[return to 192.168.56.103 \]](#)**2.2.4 Medium https (443/tcp)**

Medium (CVSS: 5.0)

NVT: PHP version smaller than 5.1.0

Summary:

PHP version smaller than 5.1.0 suffers vulnerability.

Solution:

Update PHP to version 5.1.0 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110170

References

CVE: CVE-2005-3319, CVE-2005-3883

BID:15177, 15571

Medium (CVSS: 5.0)

NVT: PHP version smaller than 5.2.9

Summary:

PHP version smaller than 5.2.9 suffers vulnerability.

Solution:

Update PHP to version 5.2.9 or later.

OID of test routine: 1.3.6.1.4.1.25623.1.0.110187

...continues on next page ...

...continued from previous page ...

References

CVE: CVE-2008-5498, CVE-2009-1271, CVE-2009-1272
 BID:33002, 33927

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers

Summary:

This routine search for weak SSL ciphers offered by a service.

Vulnerability Insight:

These rules are applied for the evaluation of the cryptographic strength:

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Weak ciphers offered by this service:

```
SSL2_RC4_128_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC2_CBC_128_CBC_WITH_MD5
SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
SSL3_RSA_RC4_40_MD5
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
SSL3_RSA_RC2_40_MD5
SSL3_RSA_DES_40_CBC_SHA
SSL3_RSA_DES_64_CBC_SHA
SSL3_EDH_RSA_DES_40_CBC_SHA
SSL3_EDH_RSA_DES_64_CBC_SHA
TLS1_RSA_RC4_40_MD5
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC2_40_MD5
```

...continues on next page ...

...continued from previous page ...

TLS1_RSA_DES_40_CBC_SHA
TLS1_RSA_DES_64_CBC_SHA
TLS1_EDH_RSA_DES_40_CBC_SHA
TLS1_EDH_RSA_DES_64_CBC_SHA

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

Medium (CVSS: 0.0)
NVT: SSL Certificate Expiry

The SSL certificate of the remote service expired on 2010-10-08 00:10:47 UTC!

OID of test routine: 1.3.6.1.4.1.25623.1.0.15901

[\[return to 192.168.56.103 \]](#)

2.2.5 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 154983160
Paket 2: 154984514

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References

Other:

URL: <http://www.ietf.org/rfc/rfc1323.txt>

[\[return to 192.168.56.103 \]](#)

2.2.6 Medium ssh (22/tcp)

Medium (CVSS: 3.5)

NVT: openssh-server Forced Command Handling Information Disclosure Vulnerability

According to its banner, the version of OpenSSH installed on the remote host is older than 5.7:

```
ssh-1.99-openssh_3.9p1
```

Summary:

The `auth_parse_options` function in `auth-options.c` in `sshd` in OpenSSH before 5.7 provides debug messages containing `authorized_keys` command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an `authorized_keys` file in its own home directory. OpenSSH before 5.7 is affected;

Solution:

Updates are available. Please see the references for more information.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103503

References

CVE: CVE-2012-0814

BID:51702

Other:

URL:<http://www.securityfocus.com/bid/51702>

URL:<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445>

URL:<http://packages.debian.org/squeeze/openssh-server>

URL:<https://downloads.avaya.com/css/P8/documents/100161262>

[\[return to 192.168.56.103 \]](#)