BAD STORE

Report generated by Nessus™ Mon, 21 Feb 2022 12:38:38 EST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

11915 (2) - Apache < 1.3.29 Multiple Modules Local Overflow

Synopsis

The remote web server is affected by multiple local buffer overflow vulnerabilities.

Description

The remote host appears to be running a version of the Apache web server which is older than 1.3.29. Such versions are reportedly affected by local buffer overflow vulnerabilities in the mod_alias and mod_rewrite modules. An attacker could exploit these vulnerabilities to execute arbitrary code in the context of the affected application.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

https://www.securityfocus.com/archive/1/342674/30/0/threaded

Solution

Upgrade to Apache web server version 1.3.29 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	8911
CVE	CVE-2003-0542
XREF	Secunia:10096
XREF	Secunia:10845
XREF	Secunia:17311
XREF	CWE:119

Plugin Information

Published: 2003/11/01, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.29
```

192.168.152.135 (tcp/443/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.29
```

15555 (2) - Apache mod_proxy Content-Length Overflow

Synopsis

The remote web server is affected by a heap-based buffer overflow vulnerability.

Description

The remote web server appears to be running a version of Apache that is older than version 1.3.32.

This version is reportedly vulnerable to a heap-based buffer overflow in proxy_util.c for mod_proxy. This issue may lead remote attackers to cause a denial of service and possibly execute arbitrary code on the server.

See Also

https://seclists.org/fulldisclosure/2004/Jun/293

https://seclists.org/fulldisclosure/2004/Jun/297

Solution

Upgrade to Apache 1.3.32 or later.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	10508
CVE	CVE-2004-0492
XREF	RHSA:2004:245
XREF	Secunia:11841
XREF	Secunia:11854
XREF	Secunia:11859
XREF	Secunia:11866
XREF	Secunia:11917
XREF	Secunia:11946

XREF	Secunia:11957
XREF	Secunia:11968
XREF	Secunia:12971
XREF	Secunia:13115

Plugin Information

Published: 2004/10/25, Modified: 2020/06/12

Plugin Output

192.168.152.135 (tcp/80/www)
192.168.152.135 (tcp/443/www)

17757 (2) - OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7l or 0.9.8d. As such, it is affected by multiple vulnerabilities :

- A remote attacker could trigger a denial of service, either via malformed ASN.1 structures or specially crafted public keys. (CVE-2006-2937, CVE-2006-3738)

- A remote attacker could execute arbitrary code on the remote server by exploiting a buffer overflow in the SSL_get_shared_ciphers function. (CVE-2006-2940)

- A remote attacker could crash a client by sending an invalid server Hello. (CVE-2006-4343)

See Also

https://www.openssl.org/news/secadv/20060928.txt

https://www.us-cert.gov/ncas/alerts/ta06-333a

Solution

Upgrade to OpenSSL 0.9.7l / 0.9.8d or later.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	20247
BID	20248
BID	20249
CVE	CVE-2006-2937
CVE	CVE-2006-3738
CVE	CVE-2006-2940

CVE	CVE-2006-4343
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7l
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7l
```

34460 (2) - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2021/11/17

Plugin Output

192.168.152.135 (tcp/80/www)

```
Product                : Apache 1.x
Server response header : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Supported versions     : Apache HTTP Server 2.4.x
Additional information : http://archive.apache.org/dist/httpd/Announcement1.3.html
```

192.168.152.135 (tcp/443/www)

```
Product                : Apache 1.x
Server response header : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Supported versions     : Apache HTTP Server 2.4.x
Additional information : http://archive.apache.org/dist/httpd/Announcement1.3.html
```

78555 (2) - OpenSSL Unsupported

Synopsis

An unsupported service is running on the remote host.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html

http://www.nessus.org/u?4d55548d

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0572

Plugin Information

Published: 2014/10/17, Modified: 2021/02/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Installed version  : 0.9.7c
Supported versions : 1.0.2 / 1.1.1 / 3.0.0
EOL URL            : https://www.openssl.org/policies/releasestrat.html
```

192.168.152.135 (tcp/443/www)

```
Installed version  : 0.9.7c
Supported versions : 1.0.2 / 1.1.1 / 3.0.0
EOL URL            : https://www.openssl.org/policies/releasestrat.html
```

153583 (2) - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.6 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/09/23, Modified: 2022/01/26

Plugin Output

192.168.152.135 (tcp/80/www)

```
URL               : http://192.168.152.135/
Installed version : 1.3.28
Fixed version     : 2.4.49
```

192.168.152.135 (tcp/443/www)

```
URL               : https://192.168.152.135/
Installed version : 1.3.28
Fixed version     : 2.4.49
```

153584 (2) - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)

- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/01/26

Plugin Output

192.168.152.135 (tcp/80/www)

```
URL               : http://192.168.152.135/
Installed version : 1.3.28
Fixed version     : 2.4.49
```

192.168.152.135 (tcp/443/www)

```
URL               : https://192.168.152.135/
Installed version : 1.3.28
Fixed version     : 2.4.49
```

12255 (2) - mod_ssl ssl_util_uuencode_binary Remote Overflow

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is using a version of mod_ssl that is older than 2.8.18.

This version is vulnerable to a flaw that could allow an attacker to disable the remote website remotely, or to execute arbitrary code on the remote host.

Note that several Linux distributions patched the old version of this module. Therefore, this alert might be a false-positive. Please check with your vendor to determine if you really are vulnerable to this flaw.

Solution

Upgrade to version 2.8.18 (Apache 1.3) or to Apache 2.0.50.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	10355
CVE	CVE-2004-0488

Plugin Information

Published: 2004/05/29, Modified: 2018/07/14

Plugin Output

192.168.152.135 (tcp/80/www)
192.168.152.135 (tcp/443/www)

13651 (2) - Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String

Synopsis

The remote web server is using a module that is affected by a remote code execution vulnerability.

Description

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

See Also

http://marc.info/?l=apache-modssl&m=109001100906749&w=2

https://marc.info/?l=bugtraq&m=109005001205991&w=2

Solution

Upgrade to mod_ssl version 2.8.19 or newer

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	10736
CVE	CVE-2004-0700

Plugin Information

Published: 2004/07/16, Modified: 2020/12/22

Plugin Output

192.168.152.135 (tcp/80/www)
192.168.152.135 (tcp/443/www)

17760 (2) - OpenSSL < 0.9.8f Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8f. As such, it is affected by the following vulnerabilities :

- A local attacker could perform a side-channel attack against the Montgomery multiplication code and retrieve RSA private keys. Note that this has not been exploited outside a laboratory environment. (CVE-2007-3108)

- A remote attacker could execute arbitrary code by exploiting an off-by-one error in the DTLS implementation. (CVE-2007-4995)

See Also

http://web.archive.org/web/20071014185140/http://cvs.openssl.org:80/chngview?cn=16275

http://www.nessus.org/u?cbc3fb3e

http://www.kb.cert.org/vuls/id/RGII-74KLP3

https://www.openssl.org/news/secadv/20071012.txt

Solution

Upgrade to OpenSSL 0.9.8f or later.

Risk Factor

High

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	25163
BID	26055
CVE	CVE-2007-3108
CVE	CVE-2007-4995

XREF	CERT:724968
XREF	CWE:189

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8f
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8f
```

31654 (2) - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

Synopsis

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

Description

The remote host appears to be running a version of Apache which is older than 1.3.37.

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

See Also

https://seclists.org/fulldisclosure/2006/Jul/671

https://www.securityfocus.com/archive//443870

Solution

Upgrade to version 1.3.37 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	19204
CVE	CVE-2006-3747
XREF	EDB-ID:3680
XREF	CWE:189

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/03/26, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.37
```

192.168.152.135 (tcp/443/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.37
```

57459 (2) - OpenSSL < 0.9.8s Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL older than 0.9.8s. Such versions have the following vulnerabilities :

- An error exists related to ECDSA signatures and binary curves. The implementation of curves over binary fields could allow a remote, unauthenticated attacker to determine private key material via timing attacks.

(CVE-2011-1945)

- The Datagram Transport Layer Security (DTLS) implementation is vulnerable to plaintext recovery attacks when decrypting in CBC mode. (CVE-2011-4108)

- A double-free error exists during a policy check failure if the flag 'X509_V_FLAG_POLICY_CHECK' is set.

(CVE-2011-4109)

- An error exists related to SSLv3.0 records that can lead to disclosure of uninitialized memory because the library does not clear all bytes used as block cipher padding. (CVE-2011-4576)

- An error exists related to RFC 3779 processing that can allow denial of service attacks. Note that this functionality is not enabled by default and must be configured at compile time via the 'enable-rfc3779'

option. (CVE-2011-4577)

- An error exists related to handshake restarts for server gated cryptography (SGC) that can allow denial of service attacks. (CVE-2011-4619)

See Also

https://www.openssl.org/news/secadv/20120104.txt

https://www.openssl.org/news/changelog.html

http://www.nessus.org/u?c0f10f36

https://eprint.iacr.org/2011/232.pdf

http://cvs.openssl.org/chngview?cn=21301

Solution

Upgrade to OpenSSL 0.9.8s or later.

Risk Factor

High

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	47888
CVE	CVE-2011-1945
CVE	CVE-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
XREF	CERT:536044

Plugin Information

Published: 2012/01/09, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8s
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8s
```

58799 (2) - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

Synopsis

The remote host may be affected by a memory corruption vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue.

Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8v was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

See Also

https://www.openssl.org/news/secadv/20120419.txt

http://seclists.org/fulldisclosure/2012/Apr/210

https://www.openssl.org/news/secadv/20120424.txt

http://cvs.openssl.org/chngview?cn=22479

https://www.openssl.org/news/changelog.html

Solution

Upgrade to OpenSSL 0.9.8w or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	53158
BID	53212
CVE	CVE-2012-2110
CVE	CVE-2012-2131
XREF	EDB-ID:18756

Plugin Information

Published: 2012/04/24, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8w
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8w
```

11213 (2) - HTTP TRACE / TRACK Methods Allowed

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.

See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604

BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

192.168.152.135 (tcp/80/www)

```
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 /Nessus1536313864.html HTTP/1.1
Connection: Close
Host: 192.168.152.135
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, 21 Feb 2022 17:20:20 GMT
Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1536313864.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
```

```
Connection: Keep-Alive
Host: 192.168.152.135
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

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

192.168.152.135 (tcp/443/www)

```


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 /Nessus1699593899.html HTTP/1.1
Connection: Close
Host: 192.168.152.135
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, 21 Feb 2022 17:20:20 GMT
Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1699593899.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 192.168.152.135
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

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

12110 (2) - OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS

Synopsis

The remote service is prone to a denial of service attack.

Description

According to its banner, the remote host is using a version of OpenSSL which is older than 0.9.6m / 0.9.7d. There are several bugs in such versions that may allow an attacker to cause a denial of service against the remote host.

See Also

https://www.openssl.org/news/secadv/20040317.txt

https://seclists.org/bugtraq/2004/Mar/155

Solution

Upgrade to version 0.9.6m / 0.9.7d or newer.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0081
CVE	CVE-2004-0112

Plugin Information

Published: 2004/03/17, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

192.168.152.135 (tcp/443/www)

17696 (2) - Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

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.

See Also

https://seclists.org/bugtraq/2008/May/109

https://seclists.org/bugtraq/2008/May/166

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.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29112
CVE	CVE-2008-2168
XREF	CWE:79

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.41
```

192.168.152.135 (tcp/443/www)

```
Version source    : Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Installed version : 1.3.28
Fixed version     : 1.3.41
```

17750 (2) - OpenSSL < 0.9.6m / 0.9.7d Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6m or 0.9.7d.

A remote attacker can crash the server by sending an overly long Kerberos ticket or a crafted SSL/TLS handshake.

See Also

https://www.us-cert.gov/ncas/alerts/ta04-078a

https://www.openssl.org/news/secadv/20040317.txt

http://marc.info/?l=bugtraq&m=107953412903636&w=2

Solution

Upgrade to OpenSSL 0.9.6m / 0.9.7d or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0112
XREF	CERT:484726

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7d
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7d
```

17755 (2) - OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback

Synopsis

The remote server is vulnerable to man-in-the-middle attacks.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7h or 0.9.8a.

If the SSL_OP_MSIE_SSLV2_RSA_PADDING option is used, a remote attacker could force a client to downgrade to a weaker protocol and implement a man-in-the-middle attack.

See Also

https://www.openssl.org/news/secadv/20051011.txt

Solution

Upgrade to OpenSSL 0.9.7h / 0.9.8a or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	15071
CVE	CVE-2005-2969

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

192.168.152.135 (tcp/80/www)

```
  Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Reported version : 0.9.7c
  Fixed version    : 0.9.7h
```

192.168.152.135 (tcp/443/www)

```
  Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Reported version : 0.9.7c
  Fixed version    : 0.9.7h
```

17756 (2) - OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability

Synopsis

The SSL layer on the remote server does not properly verify signatures.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7k or 0.9.8c.

These versions do not properly verify PKCS #1 v1.5 signatures and X509 certificates when the RSA exponent is 3.

See Also

https://www.openssl.org/news/secadv/20060905.txt

https://www.us-cert.gov/ncas/alerts/ta06-333a

Solution

Upgrade to OpenSSL 0.9.7k / 0.9.8c or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	19849
CVE	CVE-2006-4339
XREF	CERT:845620
XREF	CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7k
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.7k
```

17759 (2) - OpenSSL < 0.9.8 Weak Default Configuration

Synopsis

The default configuration of OpenSSL on the remote server uses a weak hash algorithm.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8.

The default configuration uses MD5 instead of a stronger hash algorithm. An attacker could forge certificates.

If you never generate certificates on this machine, you may ignore this warning.

See Also

https://bugs.launchpad.net/ubuntu/+source/openssl/+bug/19835

https://usn.ubuntu.com/179-1/

Solution

Upgrade to OpenSSL 0.9.8 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2005-2946
XREF	CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8
```

17761 (2) - OpenSSL < 0.9.8i Denial of Service

Synopsis

The remote server is affected by a denial of service vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8i.

A remote attacker can crash the server by sending a DTLS ChangeCipherSpec packet before the ClientHello.

See Also

http://cvs.openssl.org/chngview?cn=17369

https://rt.openssl.org/Ticket/Display.html?id=1679&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8i or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	35174
CVE	CVE-2009-1386
XREF	EDB-ID:8873

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8i
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8i
```

17762 (2) - OpenSSL < 0.9.8j Signature Spoofing

Synopsis

The remote server is affected by a signature validation bypass vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8j.

A remote attacker could implement a man-in-the-middle attack by forging an SSL/TLS signature using DSA and ECDSA keys which bypass validation of the certificate chain.

See Also

https://www.us-cert.gov/ncas/alerts/TA09-133A

Solution

Upgrade to OpenSSL 0.9.8j or later.

Risk Factor

Medium

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

References

BID	33150
CVE	CVE-2008-5077
XREF	CWE:20

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8j
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8j
```

17763 (2) - OpenSSL < 0.9.8k Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL prior to 0.9.8k. It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists in the ASN1_STRING_print_ex() function due to improper string handling. A remote attacker can exploit this to cause an invalid memory access and application crash.

(CVE-2009-0590)

- A flaw exists in the CMS_verify() function due to improper handling of errors associated with malformed signed attributes. A remote attacker can exploit this to repudiate a signature that originally appeared to be valid but was actually invalid. (CVE-2009-0591)

- A denial of service vulnerability exists due to improper handling of malformed ASN.1 structures. A remote attacker can exploit this to cause an invalid memory access and application crash. (CVE-2009-0789)

- A memory leak exists in the SSL_free() function in ssl_lib.c. A remote attacker can exploit this to exhaust memory resources, resulting in a denial of service condition. (CVE-2009-5146)

See Also

https://www.openssl.org/news/secadv/20090325.txt

Solution

Upgrade to OpenSSL version 0.9.8k or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	34256
BID	73121

CVE	CVE-2009-0590
CVE	CVE-2009-0591
CVE	CVE-2009-0789
CVE	CVE-2009-5146
XREF	CWE:119
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8k
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8k
```

17765 (2) - OpenSSL < 0.9.8l Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)

- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)

- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)

- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html

https://www.openssl.org/news/secadv/20090325.txt

http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html

https://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest

https://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest

http://cvs.openssl.org/chngview?cn=18187

http://cvs.openssl.org/chngview?cn=18188

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	EDB-ID:8720
XREF	CWE:119
XREF	CWE:189
XREF	CWE:310
XREF	CWE:399

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8l
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8l
```

56996 (2) - OpenSSL < 0.9.8h Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL older than 0.9.8h. As such, it may be affected by the following vulnerabilities :

- A double-free error exists related to the handling of server name extension data and specially crafted TLS 1.0 'Client Hello' packets. This can cause application crashes. Note that successful exploitation requires that OpenSSL is compiled with the TLS server name extensions.

(CVE-2008-0891)

- A NULL pointer dereference error exists related to anonymous Diffie-Hellman key exchange and TLS handshakes. This can be exploited by omitting the 'Server Key exchange message' from the handshake and can cause application crashes. (CVE-2008-1672)

- On 32-bit builds, an information disclosure vulnerability exists during certain calculations for NIST elliptic curves P-256 or P-384. This error can allow an attacker to recover the private key of the TLS server.

The following are required for exploitation :

- 32-bit build

- Use of elliptic curves P-256 and/or P-384

- Either the use of ECDH family ciphers and/or the use of ECDHE family ciphers without the SSL_OP_SINGLE_ECDH_USE context option

(CVE-2011-4354)

Note that Nessus has not attempted to verify that these issues are actually exploitable or have been patched but instead has relied on the version number found in the Server response header.

See Also

https://www.openwall.com/lists/oss-security/2011/12/01/6

https://www.openssl.org/news/secadv/20080528.txt

Solution

Upgrade to OpenSSL 0.9.8h or later or apply the vendor-supplied patches.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	29405
BID	50882
CVE	CVE-2008-0891
CVE	CVE-2008-1672
CVE	CVE-2011-4354
XREF	CERT:520586
XREF	CERT:661475
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2011/12/02, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8h
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8h
```

58564 (2) - OpenSSL < 0.9.8u Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses an OpenSSL version prior to 0.9.8u. As such, it is reportedly affected by the following vulnerabilities :

- An error exists in the function 'mime_hdr_cmp' that could allow a NULL pointer to be dereferenced when parsing certain MIME headers. (CVE-2006-7250)

- The fix for CVE-2011-4619 was not complete.

- An error exists in the Cryptographic Message Syntax (CMS) and PKCS #7 implementation such that data can be decrypted using Million Message Attack (MMA) adaptive chosen cipher text attack. (CVE-2012-0884)

- An error exists in the function 'mime_param_cmp' in the file 'crypto/asn1/asn_mime.c' that can allow a NULL pointer to be dereferenced when handling certain S/MIME content. (CVE-2012-1165)

Note that SSL/TLS applications are not necessarily affected, but those using CMS, PKCS #7 and S/MIME decryption operations are.

See Also

https://marc.info/?l=openssl-dev&m=115685408414194&w=2

https://www.openssl.org/news/secadv/20120312.txt

https://www.openssl.org/news/changelog.html

https://www.openwall.com/lists/oss-security/2012/03/13/2

https://www.openwall.com/lists/oss-security/2012/02/28/14

http://www.nessus.org/u?82fc5c0b

https://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8u or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	51281
BID	52181
BID	52428
BID	52764
CVE	CVE-2006-7250
CVE	CVE-2011-4619
CVE	CVE-2012-0884
CVE	CVE-2012-1165

Plugin Information

Published: 2012/04/02, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8u
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8u
```

59076 (2) - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

Synopsis

The remote host may be affected by a denial of service vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL 0.9.8 earlier than 0.9.8x. As such, the OpenSSL library itself is reportedly affected by a denial of service vulnerability.

An integer underflow error exists in the file 'ssl/d1_enc.c' in the function 'dtls1_enc'. When in CBC mode, DTLS record length values and explicit initialization vector length values related to DTLS packets are not handled properly, which can lead to memory corruption and application crashes.

See Also

https://www.openssl.org/news/secadv/20120510.txt

https://www.openssl.org/news/changelog.html

http://cvs.openssl.org/chngview?cn=22538

https://bugzilla.redhat.com/show_bug.cgi?id=820686

Solution

Upgrade to OpenSSL 0.9.8x or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	53476
CVE	CVE-2012-2333

Plugin Information

Published: 2012/05/11, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8x
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8x
```

85582 (2) - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.152.135/
  - http://192.168.152.135/cgi-bin/badstore.cgi
```

192.168.152.135 (tcp/443/www)

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - https://192.168.152.135/
  - https://192.168.152.135/cgi-bin/badstore.cgi
```

88098 (2) - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

192.168.152.135 (tcp/80/www)

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "14b-dff-44679e27"
  Inode number          : 331
  File size             : 3583 bytes
  File modification time : May. 14, 2006 at 21:16:23 GMT
```

192.168.152.135 (tcp/443/www)

```
Nessus was able to determine that the Apache Server listening on
port 443 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "14b-dff-44679e27"
  Inode number          : 331
  File size             : 3583 bytes
  File modification time : May. 14, 2006 at 21:16:23 GMT
```

40984 (1) - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following directories are browsable :

http://192.168.152.135/DoingBusiness/
http://192.168.152.135/Procedures/
http://192.168.152.135/backup/
http://192.168.152.135/images/
http://192.168.152.135/scanbot/
```

17754 (2) - OpenSSL < 0.9.7f Insecure Temporary File Creation

Synopsis

Arbitrary files could be overwritten on the remote server.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7f.

The der_chop script that is shipped with these versions allows a malicious user to overwrite arbitrary files.

Note that this was fixed in the 0.9.6 CVS but no new version was published in the 0.9.6 branch.

See Also

https://www.openssl.org/news/vulnerabilities.html#2004-0975

Solution

Upgrade to OpenSSL 0.9.7f or later.

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

BID	11293
CVE	CVE-2004-0975

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
  Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Reported version : 0.9.7c
  Fixed version    : 0.9.7f
```

192.168.152.135 (tcp/443/www)

```
  Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Reported version : 0.9.7c
  Fixed version    : 0.9.7f
```

64532 (2) - OpenSSL < 0.9.8y Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL prior to 0.9.8y. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the handling of OCSP response verification that could allow denial of service attacks.

(CVE-2013-0166)

- An error exists related to the SSL/TLS/DTLS protocols, CBC mode encryption and response time. An attacker could obtain plaintext contents of encrypted traffic via timing attacks. (CVE-2013-0169)

See Also

https://www.openssl.org/news/secadv/20130204.txt

Solution

Upgrade to OpenSSL 0.9.8y or later.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	57778
BID	60268
CVE	CVE-2013-0166
CVE	CVE-2013-0169

Plugin Information

Published: 2013/02/09, Modified: 2019/12/04

Plugin Output

192.168.152.135 (tcp/80/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8y
```

192.168.152.135 (tcp/443/www)

```
Banner           : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version : 0.9.7c
Fixed version    : 0.9.8y
```

11219 (3) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

Plugin Output

192.168.152.135 (tcp/80/www)

```
Port 80/tcp was found to be open
```

192.168.152.135 (tcp/443/www)

```
Port 443/tcp was found to be open
```

192.168.152.135 (tcp/3306)

```
Port 3306/tcp was found to be open
```

10107 (2) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

192.168.152.135 (tcp/80/www)

```
The remote web server type is :

Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
```

192.168.152.135 (tcp/443/www)

```
The remote web server type is :

Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
```

10302 (2) - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

192.168.152.135 (tcp/80/www)

```
Contents of robots.txt :

# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload
```

192.168.152.135 (tcp/443/www)

```
Contents of robots.txt :

# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload
```

10662 (2) - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

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

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2022/02/14

Plugin Output

192.168.152.135 (tcp/80/www)

```
Webmirror performed 53 queries in 1s (53.000 queries per second)

The following CGIs have been discovered :


+ CGI : /cgi-bin/badstore.cgi
  Methods : GET
  Argument : action
   Value: cartview
  Argument : searchquery


+ CGI : /
  Methods : GET
  Argument : action
   Value: search
  Argument : searchquery


+ CGI : /backup/
  Methods : GET
  Argument : D
   Value: A
  Argument : M
   Value: A
  Argument : N
```

```
    Value: D
   Argument : S
    Value: A


+ CGI : /images/
  Methods : GET
  Argument : D
   Value: A
  Argument : M
   Value: A
  Argument : N
   Value: D
  Argument : S
   Value: A


+ CGI : /scanbot/
  Methods : GET
  Argument : D
   Value: A
  Argument : M
   Value: A
  Argument : N
   Value: D
  Argument : S
   Value: A


+ CGI : /DoingBusiness/
  Methods : GET
  Argument : D
   Value: A
  Argument : M
   Value: A
  Argument : N
   Value: D
  Argument : S
   Value: A


+ CGI : /Procedures/
  Methods : GET
  Argument : D
   Value: A
  Argument : M
   Value: A
  Argument : N
   Value: D
  Argument : S
   Value: A

Directory index found at /backup/
Directory index found at /images/
Directory index found at /scanbot/
Directory index found at /DoingBusiness/
Directory index found at /Procedures/
```

192.168.152.135 (tcp/443/www)

```

Webmirror performed 20 queries in 1s (20.000 queries per second)

The following CGIs have been discovered :


+ CGI : /cgi-bin/badstore.cgi
  Methods : GET
```

```
   Argument : action
    Value: cartview
   Argument : searchquery


+ CGI : /
   Methods : GET
   Argument : action
    Value: search
   Argument : searchquery
```

11032 (2) - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

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

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following directories were discovered:
/backup, /cgi-bin, /icons, /images, //cgi-bin, //scanbot, //backup, //supplier

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

192.168.152.135 (tcp/443/www)

```
The following directories were discovered:
/backup, /cgi-bin, /icons, /images, //cgi-bin, //scanbot, //backup, //supplier

While this is not, in and of itself, a bug, you should manually inspect
```

```
these directories to ensure that they are in compliance with company
security standards
```

11419 (2) - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2021/01/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following office-related files are available on the remote server :

  - Word files (.doc) :
    /DoingBusiness/contract.doc

  - Adobe Acrobat files (.pdf) :
    /BadStore_net_v1_2_Manual.pdf
```

192.168.152.135 (tcp/443/www)

```
The following office-related files are available on the remote server :

  - Word files (.doc) :
    /DoingBusiness/contract.doc

  - Adobe Acrobat files (.pdf) :
    /BadStore_net_v1_2_Manual.pdf
```

24260 (2) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

192.168.152.135 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

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

  Date: Mon, 21 Feb 2022 17:21:30 GMT
  Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Last-Modified: Sun, 14 May 2006 21:16:23 GMT
  ETag: "14b-dff-44679e27"
  Accept-Ranges: bytes
  Content-Length: 3583
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<HTML><HEAD><TITLE>Welcome to BadStore.net v1.2.3s</TITLE></HEAD>

<BODY bgColor=#ffffff leftMargin=0 topMargin=0 MARGINHEIGHT="0" MARGINWIDTH="0">

<TABLE cellSpacing=0 cellPadding=0 width=760 bgColor=#004b2c border=0>
  <TBODY>
```

```
  <TR>
    <TD width=326 bgColor=#004b2c>
<IMG height=60 alt="BadStore.net" hspace=0 src="/images/BadStore.jpg"
width=350
border=0>
  </TD></TR></TBODY></TABLE>
<TABLE cellSpacing=0 cellPadding=0 width=760 border=0>
  <TBODY>
  <TR vAlign=top align=left>
    <TD vAlign=top width=143 bgColor=#ecece0>
      <TABLE cellSpacing=0 cellPadding=0 width=143 bgColor=#004b2c border=0>
        <FORM name=search onsubmit=/cgi-bin/badstore.cgi
        method=get>
        <TBODY>
        <TR>
          <TD vAlign=top width=143 colSpan=3>
            <TABLE cellSpacing=0 cellPadding=0 width=143 border=0>
              <TBODY>
              <TR bgColor=#004b2c>
                </TR>
              <TR vAlign=center bgColor=#004b2c width="138">
                <TD class=normal width=94 height=30> <INPUT class=normal
                  maxLength=60 size=10 name=searchquery> </TD>
<font color=yellow size=2 face=Arial><Center><B>Quick Item Search</B></Center></font>
                <TD width=44>
                  <BR><INPUT type=hidden value='search' name='action'>
                  <INPUT
                  onclick="Go Search" type=image height=25 alt="Go Search"
                  width=44
                  src="/images/index.gif"
                  border=0></A></TD></TR>
              <TR bgColor=#004b2c>
                </TR>
         [...]
```

192.168.152.135 (tcp/443/www)

```
Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : GET, HEAD, OPTIONS, TRACE
Headers :

  Date: Mon, 21 Feb 2022 17:21:31 GMT
  Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
  Last-Modified: Sun, 14 May 2006 21:16:23 GMT
  ETag: "14b-dff-44679e27"
  Accept-Ranges: bytes
  Content-Length: 3583
  Connection: close
  Content-Type: text/html

Response Body :

<HTML><HEAD><TITLE>Welcome to BadStore.net v1.2.3s</TITLE></HEAD>

<BODY bgColor=#ffffff leftMargin=0 topMargin=0 MARGINHEIGHT="0" MARGINWIDTH="0">

<TABLE cellSpacing=0 cellPadding=0 width=760 bgColor=#004b2c border=0>
  <TBODY>
  <TR>
    <TD width=326 bgColor=#004b2c>
<IMG height=60 alt="BadStore.net" hspace=0 src="/images/BadStore.jpg"
width=350
border=0>
```

```
  </TD></TR></TBODY></TABLE>
<TABLE cellSpacing=0 cellPadding=0 width=760 border=0>
  <TBODY>
  <TR vAlign=top align=left>
    <TD vAlign=top width=143 bgColor=#ecece0>
      <TABLE cellSpacing=0 cellPadding=0 width=143 bgColor=#004b2c border=0>
        <FORM name=search onsubmit=/cgi-bin/badstore.cgi
        method=get>
        <TBODY>
        <TR>
          <TD vAlign=top width=143 colSpan=3>
            <TABLE cellSpacing=0 cellPadding=0 width=143 border=0>
              <TBODY>
              <TR bgColor=#004b2c>
                </TR>
              <TR vAlign=center bgColor=#004b2c width="138">
                <TD class=normal width=94 height=30> <INPUT class=normal
                  maxLength=60 size=10 name=searchquery> </TD>
<font color=yellow size=2 face=Arial><Center><B>Quick Item Search</B></Center></font>
                <TD width=44>
                  <BR><INPUT type=hidden value='search' name='action'>
                  <INPUT
                  onclick="Go Search" type=image height=25 alt="Go Search"
                  width=44
                  src="/images/index.gif"
                  border=0></A></TD></TR>
              <TR bgColor=#004b2c>
                </TR>
              <TR>
                <TD colSpan= [...]
```

33817 (2) - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2021/01/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution (time based) : S=144        SP=144       AP=156       SC=0
 AC=156
format string                            : S=48         SP=48        AP=52        SC=0         AC=52

cross-site scripting (comprehensive test): S=96         SP=96        AP=104       SC=0
 AC=104
injectable parameter                     : S=48         SP=48        AP=52        SC=0         AC=52

arbitrary command execution              : S=384        SP=384       AP=416       SC=0
 AC=416
local file inclusion                     : S=24         SP=24        AP=26        SC=0         AC=26

directory traversal                      : S=600        SP=600       AP=650       SC=0
 AC=650
web code injection                       : S=24         SP=24        AP=26        SC=0         AC=26

blind SQL injection (4 requests)         : S=96         SP=96        AP=104       SC=0
 AC=104
```

```
persistent XSS                          : S=96         SP=96        AP=104       SC=0
 AC=104
directory traversal (write access)      : S=48         SP=48        AP=52        SC=0         AC=52

XML injection                           : S=24         SP=24        AP=26        SC=0         AC=26

blind SQL injection                     : S=288        SP=288       AP=312       SC=0
 AC=312
SQL injection                           : S=576        SP=576       AP=624       SC=0
 AC=624
directory traversal (extended test)     : S=1224       SP=1224      AP=1326      SC=0
 AC=1326
SSI injection                           : S=72         SP=72        AP=78        SC=0         AC=78

unseen parameters                       : S=840        SP=840       AP=910       SC=0
 AC=910
SQL injection (2nd order)             [...]
```

192.168.152.135 (tcp/443/www)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

injectable parameter                    : S=8          SP=8         AP=12        SC=0         AC=12

blind SQL injection (4 requests)        : S=16         SP=16        AP=24        SC=0         AC=24

arbitrary command execution (time based) : S=24        SP=24        AP=36        SC=0         AC=36

cross-site scripting (comprehensive test): S=16        SP=16        AP=24        SC=0         AC=24

directory traversal (extended test)     : S=204        SP=204       AP=306       SC=0
 AC=306
arbitrary command execution             : S=64         SP=64        AP=96        SC=0         AC=96

local file inclusion                    : S=4          SP=4         AP=6         SC=0         AC=6

web code injection                      : S=4          SP=4         AP=6         SC=0         AC=6

SQL injection                           : S=96         SP=96        AP=144       SC=0
 AC=144
directory traversal (write access)      : S=8          SP=8         AP=12        SC=0         AC=12

unseen parameters                       : S=140        SP=140       AP=210       SC=0
 AC=210
format string                           : S=8          SP=8         AP=12        SC=0         AC=12

directory traversal                     : S=100        SP=100       AP=150       SC=0
 AC=150
XML injection                           : S=4          SP=4         AP=6         SC=0         AC=6

persistent XSS                          : S=16         SP=16        AP=24        SC=0         AC=24

SSI injection                           : S=12         SP=12        AP=18        SC=0         AC=18

SQL injection (2nd order)               : S=4          SP=4         AP=6         SC=0         AC=6

blind SQL injection                   [...]
```

43111 (2) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
Based on the response to an OPTIONS request :

  - HTTP methods  HEAD  OPTIONS  POST  TRACE GET are allowed on :

    //cgi-bin
    /cgi-bin

  - HTTP methods  HEAD  OPTIONS  TRACE GET are allowed on :

    /
    //backup
    //scanbot
    //supplier
    /DoingBusiness
    /Procedures
    /backup
    /icons
    /images
    /scanbot


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    //cgi-bin
    /cgi-bin

  - HTTP methods COPY DELETE GET HEAD LOCK MKCOL MOVE OPTIONS PATCH
    POST PROPFIND PROPPATCH TRACE UNLOCK are allowed on :

    /
    //backup
    //scanbot
    //supplier
    /DoingBusiness
    /Procedures
    /backup
    /icons
    /images
    /scanbot

  - Invalid/unknown HTTP methods are allowed on :

    //cgi-bin
    /cgi-bin
```

192.168.152.135 (tcp/443/www)

```
Based on the response to an OPTIONS request :

  - HTTP methods  HEAD  OPTIONS  POST  TRACE GET are allowed on :

    //cgi-bin
    /cgi-bin

  - HTTP methods  HEAD  OPTIONS  TRACE GET are allowed on :

    /
    //backup
    //scanbot
    //supplier
```

```
    /DoingBusiness
    /Procedures
    /backup
    /icons
    /images
    /scanbot


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    //cgi-bin
    /cgi-bin

  - HTTP methods COPY DELETE GET HEAD LOCK MKCOL MOVE OPTIONS PATCH
    POST PROPFIND PROPPATCH TRACE UNLOCK are allowed on :

    /
    //backup
    //scanbot
    //supplier
    /DoingBusiness
    /Procedures
    /backup
    /icons
    /images
    /scanbot

  - Invalid/unknown HTTP methods are allowed on :

    //cgi-bin
    /cgi-bin
```

48204 (2) - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

192.168.152.135 (tcp/80/www)

```
URL        : http://192.168.152.135/
Version    : 1.3.28
backported : 0
modules    : mod_ssl/2.8.15 OpenSSL/0.9.7c
os         : Unix
```

192.168.152.135 (tcp/443/www)

```
URL        : https://192.168.152.135/
Version    : 1.3.28
backported : 0
modules    : mod_ssl/2.8.15 OpenSSL/0.9.7c
```

```
  os          : Unix
```

50344 (2) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.152.135/
  - http://192.168.152.135/DoingBusiness/
  - http://192.168.152.135/Procedures/
  - http://192.168.152.135/Procedures/UploadProc.html
  - http://192.168.152.135/backup/
  - http://192.168.152.135/cgi-bin/badstore.cgi
  - http://192.168.152.135/cgi-bin/bsheader.cgi
  - http://192.168.152.135/images/
  - http://192.168.152.135/scanbot/
```

```
  - http://192.168.152.135/scanbot/deth2botz.html
  - http://192.168.152.135/scanbot/scanbot
  - http://192.168.152.135/scanbot/scanbot.html
```

192.168.152.135 (tcp/443/www)

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://192.168.152.135/
  - https://192.168.152.135/Procedures/UploadProc.html
  - https://192.168.152.135/cgi-bin/badstore.cgi
  - https://192.168.152.135/cgi-bin/bsheader.cgi
  - https://192.168.152.135/scanbot/scanbot.html
```

50345 (2) - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.152.135/
  - http://192.168.152.135/DoingBusiness/
  - http://192.168.152.135/Procedures/
  - http://192.168.152.135/Procedures/UploadProc.html
  - http://192.168.152.135/backup/
  - http://192.168.152.135/cgi-bin/badstore.cgi
  - http://192.168.152.135/cgi-bin/bsheader.cgi
  - http://192.168.152.135/images/
  - http://192.168.152.135/scanbot/
  - http://192.168.152.135/scanbot/deth2botz.html
  - http://192.168.152.135/scanbot/scanbot
  - http://192.168.152.135/scanbot/scanbot.html
```

192.168.152.135 (tcp/443/www)

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://192.168.152.135/
  - https://192.168.152.135/Procedures/UploadProc.html
  - https://192.168.152.135/cgi-bin/badstore.cgi
  - https://192.168.152.135/cgi-bin/bsheader.cgi
  - https://192.168.152.135/scanbot/scanbot.html
```

57323 (2) - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2020/09/22

Plugin Output

192.168.152.135 (tcp/80/www)

```
Source            : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version  : 0.9.7c
```

192.168.152.135 (tcp/443/www)

```
Source            : Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Reported version  : 0.9.7c
```

91815 (2) - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

192.168.152.135 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.152.135/
  - http://192.168.152.135/BadStore_net_v1_2_Manual.pdf
  - http://192.168.152.135/DoingBusiness/
  - http://192.168.152.135/DoingBusiness/contract.doc
  - http://192.168.152.135/Procedures/
  - http://192.168.152.135/Procedures/UploadProc.html
  - http://192.168.152.135/backup/
  - http://192.168.152.135/cgi-bin/badstore.cgi
  - http://192.168.152.135/cgi-bin/bsheader.cgi
  - http://192.168.152.135/images/
  - http://192.168.152.135/images/1000.jpg
  - http://192.168.152.135/images/1001.jpg
  - http://192.168.152.135/images/1002.jpg
  - http://192.168.152.135/images/1003.jpg
  - http://192.168.152.135/images/1004.jpg
  - http://192.168.152.135/images/1005.jpg
  - http://192.168.152.135/images/1006.jpg
  - http://192.168.152.135/images/1007.jpg
  - http://192.168.152.135/images/1008.jpg
  - http://192.168.152.135/images/1009.jpg
  - http://192.168.152.135/images/1010.jpg
```

```
  - http://192.168.152.135/images/1011.jpg
  - http://192.168.152.135/images/1012.jpg
  - http://192.168.152.135/images/1013.jpg
  - http://192.168.152.135/images/1014.jpg
  - http://192.168.152.135/images/9999.jpg
  - http://192.168.152.135/images/BadStore.jpg
  - http://192.168.152.135/images/amex.jpg
  - http://192.168.152.135/images/bucket.jpg
  - http://192.168.152.135/images/cart.jpg
  - http://192.168.152.135/images/discover.jpg
  - http://192.168.152.135/images/index.gif
  - http://192.168.152.135/images/mastercard.jpg
  - http://192.168.152.135/images/seal.jpg
  - http://192.168.152.135/images/store1.jpg
  - http://192.168.152.135/images/visa.jpg
  - http://192.168.152.135/scanbot/
  - http://192.168.152.135/scanbot/deth2botz.html
  - http://192.168.152.135/scanbot/scanbot
  - http://192.168.152.135/scanbot/scanbot.html

Attached is a copy of the sitemap file.
```

192.168.152.135 (tcp/443/www)

```
The following sitemap was created from crawling linkable content on the target host :

  - https://192.168.152.135/
  - https://192.168.152.135/BadStore_net_v1_2_Manual.pdf
  - https://192.168.152.135/DoingBusiness/contract.doc
  - https://192.168.152.135/Procedures/UploadProc.html
  - https://192.168.152.135/cgi-bin/badstore.cgi
  - https://192.168.152.135/cgi-bin/bsheader.cgi
  - https://192.168.152.135/scanbot/scanbot.html

Attached is a copy of the sitemap file.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

192.168.152.135 (tcp/0)

```
Information about this scan :

Nessus version : 10.1.1
Nessus build : X20061
Plugin feed version : 202202200611
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
```

```
Scan name : BAD STORE
Scan policy used : Web Application Tests
Scanner IP : 192.168.152.132
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 151.469 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/2/21 12:18 EST
Scan duration : 1212 sec
```

49704 (1) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

192.168.152.135 (tcp/80/www)

```
3 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://backup/                          - //backup
http://scanbot/                         - //scanbot
http://supplier/                        - //supplier
```

84502 (1) - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

192.168.152.135 (tcp/443/www)

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```