Ethical non-intrusive scan of Zero Bank

Report generated by Tenable Nessus™ Tue, 10 Feb 2026 12:49:39 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

ec2-54-82-22-214.compute-1.amazonaws.com

30	46	34	2	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	ec2-54-82-22-214.compute-1.amazonaws.com
IP:	54.82.22.214
OS:	Microsoft Windows Vista

Vulnerabilities

57603 - Apache 2.2.x < 2.2.13 APR apr_palloc Heap Overflow

Synopsis

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

Description

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

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

See Also

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

Solution

Upgrade to Apache 2.2.13 or later.

Risk Factor

Critical

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)

VPR Score

6.7

EPSS Score

0.0556

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	35949
CVE	CVE-2009-2412
XREF	CWE:189

Plugin Information

Published: 2012/01/19, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.13
```

45004 - Apache 2.2.x < 2.2.15 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :

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

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

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

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

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

See Also

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

https://bz.apache.org/bugzilla/show_bug.cgi?id=48359

https://archive.apache.org/dist/httpd/CHANGES_2.2.15

Solution

Upgrade to Apache version 2.2.15 or later.

Risk Factor

Critical

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

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

VPR Score

9.0

EPSS Score

0.8682

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

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

References

BID	21865
BID	36935
BID	38491
BID	38494
BID	38580
CVE	CVE-2007-6750
CVE	CVE-2009-3555
CVE	CVE-2010-0408
CVE	CVE-2010-0425
CVE	CVE-2010-0434
XREF	Secunia:38776
XREF	CWE:200
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2010/10/20, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.15
```

100995 - Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x.

(CVE-2017-7659)

- An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition.

(CVE-2017-7668)

- An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679)

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.32

https://archive.apache.org/dist/httpd/CHANGES_2.4.26

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

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

Solution

Upgrade to Apache version 2.2.33-dev / 2.4.26 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

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

VPR Score

6.7

EPSS Score

0.6441

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	99132
BID	99134
BID	99135
BID	99137
BID	99170
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7659
CVE	CVE-2017-7668
CVE	CVE-2017-7679

Plugin Information

Published: 2017/06/22, Modified: 2025/12/15

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.2.33
```

101787 - Apache 2.2.x < 2.2.34 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :

- An authentication bypass vulnerability exists in httpd due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167)

- A denial of service vulnerability exists in httpd due to a NULL pointer dereference flaw that is triggered when a third-party module calls the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the ap_find_token() function that is triggered when handling a specially crafted request header sequence. An unauthenticated, remote attacker can exploit this to crash the service or force ap_find_token() to return an incorrect value. (CVE-2017-7668)

- A denial of service vulnerability exists in httpd due to an out-of-bounds read error in the mod_mime that is triggered when handling a specially crafted Content-Type response header. An unauthenticated, remote attacker can exploit this to disclose sensitive information or cause a denial of service condition. (CVE-2017-7679)

- A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '='

assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788)

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.34

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

Solution

Upgrade to Apache version 2.2.34 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

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

VPR Score

6.7

EPSS Score

0.6441

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	99134
BID	99135
BID	99137
BID	99170
BID	99569
CVE	CVE-2017-3167
CVE	CVE-2017-3169
CVE	CVE-2017-7668
CVE	CVE-2017-7679
CVE	CVE-2017-9788

Plugin Information

Published: 2017/07/18, Modified: 2025/12/10

Plugin Output

tcp/443/www

```
  Source            : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
```

```
    Fixed version     : 2.2.34
```

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

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

See Also

http://www.apache.org/dist/httpd/Announcement2.4.html

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

Solution

Upgrade to Apache version 2.4.53 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

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

VPR Score

6.7

EPSS Score

0.6805

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)

STIG Severity

I

References

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XREF	IAVA:2022-A-0124-S

Plugin Information

Published: 2022/03/14, Modified: 2023/11/06

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.53
```

193421 - Apache 2.4.x < 2.4.54 Authentication Bypass

Synopsis

The remote web server is affected by an authentication bypass vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by an authentication bypass vulnerability as referenced in the 2.4.54 advisory.

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 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)

VPR Score

6.7

EPSS Score

0.0004

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-2022-31813
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.54
```

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0103

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-28614
CVE	CVE-2022-28615
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2022/06/08, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.54
```

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
(CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

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

Solution

Upgrade to Apache version 2.4.55 or later.

Risk Factor

High

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

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

VPR Score

7.3

EPSS Score

0.2314

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2006-20001
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XREF	IAVA:2023-A-0047-S

Plugin Information

Published: 2023/01/18, Modified: 2023/03/10

Plugin Output

tcp/443/www

```
URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 2.2.6
Fixed version     : 2.4.55
```

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

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

Solution

Upgrade to Apache version 2.4.56 or later.

Risk Factor

Critical

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

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

VPR Score

6.7

EPSS Score

0.6704

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)

STIG Severity

I

References

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XREF	IAVA:2023-A-0124-S

Plugin Information

Published: 2023/03/07, Modified: 2023/10/21

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.56
```

153583 - 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

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

VPR Score

8.1

EPSS Score

0.9443

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

5.6 (CVSS2#E:F/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: 2023/04/25

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.49
```

153584 - 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)

VPR Score

7.4

EPSS Score

0.4419

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: 2022/04/11

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.49
```

171356 - Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)

Synopsis

An unsupported version of Apache HTTP Server is installed on the remote host.

Description

According to its version, Apache HTTP Server is between 2.1.x and 2.2.x. It is, therefore, 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.

See Also

https://archive.apache.org/dist/httpd/Announcement2.2.txt

Solution

Upgrade to a version of Apache HTTP Server 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)

Plugin Information

Published: 2023/02/10, Modified: 2024/04/02

Plugin Output

tcp/443/www

```
URL                                   : https://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version                     : 2.2.6
Security End of Life                  : July 11, 2017
Time since Security End of Life (Est.) : >= 8 years
```

197843 - Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.100. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.100_security-7 advisory.

- When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

(CVE-2020-1938)

- In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2020-1935)

- The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2019-17569)

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

See Also

http://www.nessus.org/u?f7ee9495

http://www.nessus.org/u?074f4bcc

http://www.nessus.org/u?da2f8a53

http://www.nessus.org/u?8dd243d1

http://www.nessus.org/u?e21417cd

http://www.nessus.org/u?ceb9dcd0

http://www.nessus.org/u?8ebe6246

Solution

Upgrade to Apache Tomcat version 7.0.100 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

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

VPR Score

8.9

EPSS Score

0.9447

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

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

References

CVE	CVE-2019-17569
CVE	CVE-2020-1935
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```

  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.100
```

197843 - Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.100. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.100_security-7 advisory.

- When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

(CVE-2020-1938)

- In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2020-1935)

- The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2019-17569)

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

See Also

http://www.nessus.org/u?f7ee9495

http://www.nessus.org/u?074f4bcc

http://www.nessus.org/u?da2f8a53

http://www.nessus.org/u?8dd243d1

http://www.nessus.org/u?e21417cd

http://www.nessus.org/u?ceb9dcd0

http://www.nessus.org/u?8ebe6246

Solution

Upgrade to Apache Tomcat version 7.0.100 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

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

VPR Score

8.9

EPSS Score

0.9447

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

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

References

CVE	CVE-2019-17569
CVE	CVE-2020-1935
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.100
```

197818 - Apache Tomcat 7.0.0 < 7.0.72 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.72. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.72_security-7 advisory.

- The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not. (CVE-2016-6797)

- A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet. (CVE-2016-6796)

- When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible. (CVE-2016-6794)

- In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications. (CVE-2016-5018)

- The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.

(CVE-2016-0762)

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

See Also

https://svn.apache.org/viewvc?view=rev&rev=1757275

https://svn.apache.org/viewvc?view=rev&rev=1758495

https://svn.apache.org/viewvc?view=rev&rev=1763236

https://svn.apache.org/viewvc?view=rev&rev=1754728

https://svn.apache.org/viewvc?view=rev&rev=1754902

https://svn.apache.org/viewvc?view=rev&rev=1760309

https://svn.apache.org/viewvc?view=rev&rev=1758502

http://www.nessus.org/u?be50738a

Solution

Upgrade to Apache Tomcat version 7.0.72 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0105

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-0762
CVE	CVE-2016-5018
CVE	CVE-2016-6794
CVE	CVE-2016-6796
CVE	CVE-2016-6797

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.72
```

197818 - Apache Tomcat 7.0.0 < 7.0.72 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.72. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.72_security-7 advisory.

- The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not. (CVE-2016-6797)

- A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet. (CVE-2016-6796)

- When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible. (CVE-2016-6794)

- In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications. (CVE-2016-5018)

- The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.

(CVE-2016-0762)

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

See Also

https://svn.apache.org/viewvc?view=rev&rev=1757275

https://svn.apache.org/viewvc?view=rev&rev=1758495

https://svn.apache.org/viewvc?view=rev&rev=1763236

https://svn.apache.org/viewvc?view=rev&rev=1754728

https://svn.apache.org/viewvc?view=rev&rev=1754902

https://svn.apache.org/viewvc?view=rev&rev=1760309

https://svn.apache.org/viewvc?view=rev&rev=1758502

http://www.nessus.org/u?be50738a

Solution

Upgrade to Apache Tomcat version 7.0.72 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0105

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-0762
CVE	CVE-2016-5018
CVE	CVE-2016-6794
CVE	CVE-2016-6796
CVE	CVE-2016-6797

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.72
```

197848 - Apache Tomcat 7.0.0 < 7.0.73 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.73. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.73_security-7 advisory.

- Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types. (CVE-2016-8735)

- The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own. (CVE-2016-6816)

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

See Also

https://svn.apache.org/viewvc?view=rev&rev=1767676

https://svn.apache.org/viewvc?view=rev&rev=1767675

http://www.nessus.org/u?1c7e7b23

Solution

Upgrade to Apache Tomcat version 7.0.73 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

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

VPR Score

7.4

EPSS Score

0.9367

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

CVE	CVE-2016-6816
CVE	CVE-2016-8735
CVE	CVE-2016-8735
XREF	CISA-KNOWN-EXPLOITED:2023/06/02

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.73
```

197848 - Apache Tomcat 7.0.0 < 7.0.73 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.73. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.73_security-7 advisory.

- Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types. (CVE-2016-8735)

- The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own. (CVE-2016-6816)

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

See Also

https://svn.apache.org/viewvc?view=rev&rev=1767676

https://svn.apache.org/viewvc?view=rev&rev=1767675

http://www.nessus.org/u?1c7e7b23

Solution

Upgrade to Apache Tomcat version 7.0.73 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

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

VPR Score

7.4

EPSS Score

0.9367

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

CVE	CVE-2016-6816
CVE	CVE-2016-8735
CVE	CVE-2016-8735
XREF	CISA-KNOWN-EXPLOITED:2023/06/02

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.73
```

121120 - Apache Tomcat 7.0.0 < 7.0.76

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.76. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.76_security-7 advisory.

- While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application. (CVE-2017-5648)

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

See Also

http://www.nessus.org/u?839fc4af

https://svn.apache.org/viewvc?view=rev&rev=1785777

Solution

Upgrade to Apache Tomcat version 7.0.76 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.19

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-5648

Plugin Information

Published: 2019/01/11, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.76
```

121120 - Apache Tomcat 7.0.0 < 7.0.76

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.76. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.76_security-7 advisory.

- While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application. (CVE-2017-5648)

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

See Also

http://www.nessus.org/u?839fc4af

https://svn.apache.org/viewvc?view=rev&rev=1785777

Solution

Upgrade to Apache Tomcat version 7.0.76 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.19

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2017-5648

Plugin Information

Published: 2019/01/11, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.76
```

111066 - Apache Tomcat 7.0.0 < 7.0.89

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.89. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.89_security-7 advisory.

- The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, 7.0.41 to 7.0.88 are insecure and enable 'supportsCredentials' for all origins. It is expected that users of the CORS filter will have configured it appropriately for their environment rather than using it in the default configuration. Therefore, it is expected that most users will not be impacted by this issue. (CVE-2018-8014)

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

See Also

http://www.nessus.org/u?8757ab94

https://svn.apache.org/viewvc?view=rev&rev=1831730

Solution

Upgrade to Apache Tomcat version 7.0.89 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)

VPR Score

6.7

EPSS Score

0.4879

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	104203
CVE	CVE-2018-8014

Plugin Information

Published: 2018/07/24, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.89
```

111066 - Apache Tomcat 7.0.0 < 7.0.89

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.89. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.89_security-7 advisory.

- The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, 7.0.41 to 7.0.88 are insecure and enable 'supportsCredentials' for all origins. It is expected that users of the CORS filter will have configured it appropriately for their environment rather than using it in the default configuration. Therefore, it is expected that most users will not be impacted by this issue. (CVE-2018-8014)

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

See Also

http://www.nessus.org/u?8757ab94

https://svn.apache.org/viewvc?view=rev&rev=1831730

Solution

Upgrade to Apache Tomcat version 7.0.89 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)

VPR Score

6.7

EPSS Score

0.4879

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	104203
CVE	CVE-2018-8014

Plugin Information

Published: 2018/07/24, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.89
```

171351 - Apache Tomcat SEoL (7.0.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is 7.0.x. It is, therefore, 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.

See Also

https://tomcat.apache.org/tomcat-70-eol.html

Solution

Upgrade to a version of Apache Tomcat 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)

Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

Plugin Output

tcp/80/www

```
  URL                                     : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version                       : 7.0.70
  Security End of Life                    : March 31, 2021
  Time since Security End of Life (Est.) : >= 4 years
```

171351 - Apache Tomcat SEoL (7.0.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is 7.0.x. It is, therefore, 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.

See Also

https://tomcat.apache.org/tomcat-70-eol.html

Solution

Upgrade to a version of Apache Tomcat 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)

Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

Plugin Output

tcp/8080/www

```
URL                                    : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version                      : 7.0.70
Security End of Life                   : March 31, 2021
Time since Security End of Life (Est.) : >= 4 years
```

17760 - OpenSSL 0.9.8 < 0.9.8f Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8f. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8f advisory.

- Off-by-one error in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 up to 0.9.7l, and 0.9.8 up to 0.9.8f, might allow remote attackers to execute arbitrary code via a crafted packet that triggers a one- byte buffer underflow. NOTE: this issue was introduced as a result of a fix for CVE-2006-3738. As of 20071012, it is unknown whether code execution is possible. (CVE-2007-5135)

- Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors. (CVE-2007-4995)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2007-4995

https://www.cve.org/CVERecord?id=CVE-2007-5135

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

Solution

Upgrade to OpenSSL version 0.9.8f 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)

VPR Score

5.9

EPSS Score

0.4752

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-2007-4995
CVE	CVE-2007-5135
XREF	CERT:724968

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8f
```

45039 - OpenSSL 0.9.8 < 0.9.8m Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8m. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8m advisory.

- OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors. (CVE-2009-3245)

- Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678. (CVE-2009-4355)

- The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a plaintext injection attack, aka the Project Mogul issue. (CVE-2009-3555)

- Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate. (CVE-2009-1379)

- Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka DTLS fragment handling memory leak. (CVE-2009-1378)

- The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of future epoch DTLS records that are buffered in a queue, aka DTLS record buffer limitation bug. (CVE-2009-1377)

- The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a fragment bug. (CVE-2009-1387)

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

See Also

http://www.nessus.org/u?0b059be1

http://www.nessus.org/u?3c9c6054

http://www.nessus.org/u?66b78730

http://www.nessus.org/u?8017a0da

http://www.nessus.org/u?81086b9d

http://www.nessus.org/u?b1dd7a8e

http://www.nessus.org/u?be95a7f1

http://www.nessus.org/u?c95727f2

http://www.nessus.org/u?f79b6f49

https://www.cve.org/CVERecord?id=CVE-2009-1377

https://www.cve.org/CVERecord?id=CVE-2009-1378

https://www.cve.org/CVERecord?id=CVE-2009-1379

https://www.cve.org/CVERecord?id=CVE-2009-1387

https://www.cve.org/CVERecord?id=CVE-2009-3245

https://www.cve.org/CVERecord?id=CVE-2009-3555

https://www.cve.org/CVERecord?id=CVE-2009-4355

https://www.openssl.org/news/secadv/20091111.txt

Solution

Upgrade to OpenSSL version 0.9.8m or later.

Risk Factor

Critical

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

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

VPR Score

7.4

EPSS Score

0.2024

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	31692
BID	36935
BID	38562
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-1379
CVE	CVE-2009-1387
CVE	CVE-2009-3245
CVE	CVE-2009-3555
CVE	CVE-2009-4355
XREF	Secunia:37291
XREF	Secunia:38200

Plugin Information

Published: 2010/03/11, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8m
```

200190 - OpenSSL 0.9.8 < 0.9.8p Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8p. It is, therefore, affected by a vulnerability as referenced in the 0.9.8p advisory.

- Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography. (CVE-2010-3864)

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://www.cve.org/CVERecord?id=CVE-2010-3864

https://www.openssl.org/news/secadv/20101116.txt

Solution

Upgrade to OpenSSL version 0.9.8p 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)

VPR Score

5.9

EPSS Score

0.0736

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2010-3864
XREF	IAVA:2010-A-0166-S

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8p
```

57459 - OpenSSL 0.9.8 < 0.9.8s Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8s. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8s advisory.

- The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication. (CVE-2015-1788)

- The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors. (CVE-2011-4619)

- OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers. (CVE-2011-4577)

- The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer. (CVE-2011-4576)

- Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check. (CVE-2011-4109)

- The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack. (CVE-2011-4108)

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

See Also

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

https://www.openssl.org/news/secadv/20150611.txt

https://www.cve.org/CVERecord?id=CVE-2011-4108

https://www.cve.org/CVERecord?id=CVE-2011-4109

https://www.cve.org/CVERecord?id=CVE-2011-4576

https://www.cve.org/CVERecord?id=CVE-2011-4577

https://www.cve.org/CVERecord?id=CVE-2011-4619

https://www.cve.org/CVERecord?id=CVE-2015-1788

Solution

Upgrade to OpenSSL version 0.9.8s 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)

VPR Score

5.9

EPSS Score

0.2014

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-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
CVE	CVE-2015-1788
XREF	CERT:536044

Plugin Information

Published: 2012/01/09, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8s
```

58799 - OpenSSL 0.9.8 < 0.9.8v Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8v. It is, therefore, affected by a vulnerability as referenced in the 0.9.8v advisory.

- The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

(CVE-2012-2110)

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

https://www.cve.org/CVERecord?id=CVE-2012-2110

Solution

Upgrade to OpenSSL version 0.9.8v 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

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

VPR Score

6.7

EPSS Score

0.0628

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
XREF	EDB-ID:18756

Plugin Information

Published: 2012/04/24, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8v
```

78552 - OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zc. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8zc advisory.

- OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c. (CVE-2014-3568)

- Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure. (CVE-2014-3567)

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

See Also

https://www.openssl.org/news/secadv/20141015.txt

https://www.cve.org/CVERecord?id=CVE-2014-3567

https://www.cve.org/CVERecord?id=CVE-2014-3568

Solution

Upgrade to OpenSSL version 0.9.8zc or later.

Risk Factor

Medium

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)

VPR Score

3.6

EPSS Score

0.2024

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

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

References

BID	70574
BID	70585
BID	70586
CVE	CVE-2014-3567
CVE	CVE-2014-3568
XREF	CERT:577193

Plugin Information

Published: 2014/10/17, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8zc
```

40467 - Apache 2.2.x < 2.2.12 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x. running on the remote host is prior to 2.2.12. It is, therefore, affected by the following vulnerabilities :

- A heap-based buffer underwrite flaw exists in the function 'apr_strmatch_precompile()' in the bundled copy of the APR-util library, which could be triggered when parsing configuration data to crash the daemon.

(CVE-2009-0023)

- A flaw in the mod_proxy_ajp module in version 2.2.11 only may allow a remote attacker to obtain sensitive response data intended for a client that sent an earlier POST request with no request body.

(CVE-2009-1191)

- The server does not limit the use of directives in a .htaccess file as expected based on directives such as 'AllowOverride' and 'Options' in the configuration file, which could enable a local user to bypass security restrictions. (CVE-2009-1195)

- Failure to properly handle an amount of streamed data that exceeds the Content-Length value allows a remote attacker to force a proxy process to consume CPU time indefinitely when mod_proxy is used in a reverse proxy configuration. (CVE-2009-1890)

- Failure of mod_deflate to stop compressing a file when the associated network connection is closed may allow a remote attacker to consume large amounts of CPU if there is a large (>10 MB) file available that has mod_deflate enabled. (CVE-2009-1891)

- Using a specially crafted XML document with a large number of nested entities, a remote attacker may be able to consume an excessive amount of memory due to a flaw in the bundled expat XML parser used by the mod_dav and mod_dav_svn modules. (CVE-2009-1955)

- There is an off-by-one overflow in the function 'apr_brigade_vprintf()' in the bundled copy of the APR-util library in the way it handles a variable list of arguments, which could be leveraged on big-endian platforms to perform information disclosure or denial of service attacks. (CVE-2009-1956)

Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use.

See Also

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

Solution

Upgrade to Apache version 2.2.12 or later. Alternatively, ensure that the affected modules / directives are not in use.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.4

EPSS Score

0.2156

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	34663
BID	35115
BID	35221
BID	35251
BID	35253
BID	35565
BID	35623
CVE	CVE-2009-0023
CVE	CVE-2009-1191
CVE	CVE-2009-1195
CVE	CVE-2009-1890
CVE	CVE-2009-1891
CVE	CVE-2009-1955
CVE	CVE-2009-1956
XREF	CWE:16
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2009/08/02, Modified: 2020/04/27

Plugin Output

tcp/443/www

```

  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.12
```

42052 - Apache 2.2.x < 2.2.14 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.14. It is, therefore, potentially affected by multiple vulnerabilities :

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

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

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

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

See Also

http://www.securityfocus.com/advisories/17947

http://www.securityfocus.com/advisories/17959

http://www.nessus.org/u?e470f137

https://bz.apache.org/bugzilla/show_bug.cgi?id=47645

http://www.nessus.org/u?c34c4eda

Solution

Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use.

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

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

VPR Score

6.7

EPSS Score

0.0873

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	36254
BID	36260
BID	36596
CVE	CVE-2009-2699
CVE	CVE-2009-3094
CVE	CVE-2009-3095
XREF	Secunia:36549
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2009/10/07, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.14
```

62101 - Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars' file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution.
(CVE-2012-0883)

- An input validation error exists related to 'mod_negotiation', 'Multiviews' and untrusted uploads that can allow cross-site scripting attacks.
(CVE-2012-2687)

Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.23

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

Solution

Upgrade to Apache version 2.2.23 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0732

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53046
BID	55131
CVE	CVE-2012-0883
CVE	CVE-2012-2687
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/09/14, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.23
```

77531 - Apache 2.2.x < 2.2.28 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the 'mod_headers' module which allows a remote attacker to inject arbitrary headers.

This is done by placing a header in the trailer portion of data being sent using chunked transfer encoding.

(CVE-2013-5704)

- A flaw exists within the 'mod_deflate' module when handling highly compressed bodies. Using a specially crafted request, a remote attacker can exploit this to cause a denial of service by exhausting memory and CPU resources. (CVE-2014-0118)

- The 'mod_status' module contains a race condition that can be triggered when handling the scoreboard. A remote attacker can exploit this to cause a denial of service, execute arbitrary code, or obtain sensitive credential information. (CVE-2014-0226)

- The 'mod_cgid' module lacks a time out mechanism. Using a specially crafted request, a remote attacker can use this flaw to cause a denial of service by causing child processes to linger indefinitely, eventually filling up the scoreboard. (CVE-2014-0231)

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

See Also

https://www.zerodayinitiative.com/advisories/ZDI-14-236/

https://archive.apache.org/dist/httpd/CHANGES_2.2.29

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

http://swende.se/blog/HTTPChunked.html

Solution

Upgrade to Apache version 2.2.29 or later.

Note that version 2.2.28 was never officially released.

Risk Factor

Medium

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

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

VPR Score

6.7

EPSS Score

0.7544

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

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

References

BID	66550
BID	68678
BID	68742
BID	68745
CVE	CVE-2013-5704
CVE	CVE-2014-0118
CVE	CVE-2014-0226
CVE	CVE-2014-0231
XREF	EDB-ID:34133

Plugin Information

Published: 2014/09/04, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.29
```

193422 - Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability

Synopsis

The remote web server is affected by a HTTP request smuggling vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by a http request smuggling vulnerability as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.393

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)

STIG Severity

I

References

CVE	CVE-2022-26377
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.54
```

193423 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.1194

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)

STIG Severity

I

References

CVE	CVE-2022-30522
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.54
```

193424 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0215

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)

STIG Severity

I

References

CVE	CVE-2022-29404
CVE	CVE-2022-30556
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.54
```

183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. Acknowledgements: (CVE-2023-45802)

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

Solution

Upgrade to Apache version 2.4.58 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.5906

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-43622
CVE	CVE-2023-45802
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2023/10/19, Modified: 2024/04/29

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.58
```

193419 - Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)

Synopsis

The remote web server is affected by an out-of-bounds read vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57.

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

Solution

Upgrade to Apache version 2.4.58 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0035

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-31122
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/29

Plugin Output

tcp/443/www

```
URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 2.2.6
Fixed version     : 2.4.58
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/) (CVE-2024-27316)

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

Solution

Upgrade to Apache version 2.4.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.8912

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-38709
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/04/04, Modified: 2024/07/12

Plugin Output

tcp/443/www

```
  URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 2.2.6
  Fixed version     : 2.4.59
```

136770 - Apache Tomcat 7.0.0 < 7.0.104

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.104. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.104_security-7 advisory.

- When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter=null (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed. (CVE-2020-9484)

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

See Also

http://www.nessus.org/u?d383947b

Solution

Upgrade to Apache Tomcat version 7.0.104 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.9333

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-9484
XREF	IAVA:2020-A-0225-S
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/05/22, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.104
```

136770 - Apache Tomcat 7.0.0 < 7.0.104

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.104. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.104_security-7 advisory.

- When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter=null (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed. (CVE-2020-9484)

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

See Also

http://www.nessus.org/u?d383947b

Solution

Upgrade to Apache Tomcat version 7.0.104 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.9333

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-9484
XREF	IAVA:2020-A-0225-S
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/05/22, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.104
```

147163 - Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.108. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.108_security-7 advisory.

- The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue. (CVE-2021-25329)

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

See Also

http://www.nessus.org/u?e5b3746f

http://www.nessus.org/u?b7d039d2

Solution

Upgrade to Apache Tomcat version 7.0.108 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-25329
XREF	IAVA:2021-A-0114-S

Plugin Information

Published: 2021/03/05, Modified: 2024/05/24

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.108
```

147163 - Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.108. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.108_security-7 advisory.

- The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue. (CVE-2021-25329)

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

See Also

http://www.nessus.org/u?e5b3746f

http://www.nessus.org/u?b7d039d2

Solution

Upgrade to Apache Tomcat version 7.0.108 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-25329
XREF	IAVA:2021-A-0114-S

Plugin Information

Published: 2021/03/05, Modified: 2024/05/24

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.108
```

197823 - Apache Tomcat 7.0.0 < 7.0.75

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.75. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.75_security-7 advisory.

- A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions. (CVE-2016-8745)

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://svn.apache.org/viewvc?view=rev&rev=1777471

http://www.nessus.org/u?8e9b7a2b

Solution

Upgrade to Apache Tomcat version 7.0.75 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.171

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

CVE	CVE-2016-8745

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.75
```

197823 - Apache Tomcat 7.0.0 < 7.0.75

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.75. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.75_security-7 advisory.

- A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions. (CVE-2016-8745)

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://svn.apache.org/viewvc?view=rev&rev=1777471

http://www.nessus.org/u?8e9b7a2b

Solution

Upgrade to Apache Tomcat version 7.0.75 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.171

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

CVE	CVE-2016-8745

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.75
```

197820 - Apache Tomcat 7.0.0 < 7.0.77

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.77. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.77_security-7 advisory.

- A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. (CVE-2017-5647)

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://svn.apache.org/viewvc?view=rev&rev=1789008

http://www.nessus.org/u?5c93fea8

Solution

Upgrade to Apache Tomcat version 7.0.77 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0268

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

CVE	CVE-2017-5647

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.77
```

197820 - Apache Tomcat 7.0.0 < 7.0.77

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.77. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.77_security-7 advisory.

- A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. (CVE-2017-5647)

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://svn.apache.org/viewvc?view=rev&rev=1789008

http://www.nessus.org/u?5c93fea8

Solution

Upgrade to Apache Tomcat version 7.0.77 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0268

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

CVE	CVE-2017-5647

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.77
```

197831 - Apache Tomcat 7.0.0 < 7.0.78

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.78. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.78_security-7 advisory.

- The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method.

If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page.

Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (CVE-2017-5664)

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://svn.apache.org/viewvc?view=rev&rev=1793471

https://svn.apache.org/viewvc?view=rev&rev=1793491

http://www.nessus.org/u?de5925ac

Solution

Upgrade to Apache Tomcat version 7.0.78 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0957

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-2017-5664

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.78
```

197831 - Apache Tomcat 7.0.0 < 7.0.78

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.78. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.78_security-7 advisory.

- The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method.

If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page.

Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (CVE-2017-5664)

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://svn.apache.org/viewvc?view=rev&rev=1793471

https://svn.apache.org/viewvc?view=rev&rev=1793491

http://www.nessus.org/u?de5925ac

Solution

Upgrade to Apache Tomcat version 7.0.78 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0957

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-2017-5664

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.78
```

103329 - Apache Tomcat 7.0.0 < 7.0.81 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.81. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.81_security-7 advisory.

- When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request. (CVE-2017-12616)

- When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12615)

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

See Also

http://www.nessus.org/u?58d5675a

https://svn.apache.org/viewvc?view=rev&rev=1804604

https://svn.apache.org/viewvc?view=rev&rev=1804729

Solution

Upgrade to Apache Tomcat version 7.0.81 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.9422

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)

References

BID	100897
BID	100901
CVE	CVE-2017-12615
CVE	CVE-2017-12616
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

CANVAS (true) (true)

Plugin Information

Published: 2017/09/19, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.81
```

103329 - Apache Tomcat 7.0.0 < 7.0.81 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.81. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.81_security-7 advisory.

- When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request. (CVE-2017-12616)

- When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12615)

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

See Also

http://www.nessus.org/u?58d5675a

https://svn.apache.org/viewvc?view=rev&rev=1804604

https://svn.apache.org/viewvc?view=rev&rev=1804729

Solution

Upgrade to Apache Tomcat version 7.0.81 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.9422

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)

References

BID	100897
BID	100901
CVE	CVE-2017-12615
CVE	CVE-2017-12616
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

CANVAS (true) (true)

Plugin Information

Published: 2017/09/19, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.81
```

103782 - Apache Tomcat 7.0.0 < 7.0.82

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.82. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.82_security-7 advisory.

- When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12617)

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

See Also

http://www.nessus.org/u?0d247a3f

https://svn.apache.org/viewvc?view=rev&rev=1809978

https://svn.apache.org/viewvc?view=rev&rev=1809992

https://svn.apache.org/viewvc?view=rev&rev=1810014

https://svn.apache.org/viewvc?view=rev&rev=1810026

Solution

Upgrade to Apache Tomcat version 7.0.82 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.9436

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)

References

BID	100954
CVE	CVE-2017-12617
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CEA-ID:CEA-2019-0240

Exploitable With

Core Impact (true) (true) Metasploit (true)

Plugin Information

Published: 2017/10/11, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.82
```

103782 - Apache Tomcat 7.0.0 < 7.0.82

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.82. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.82_security-7 advisory.

- When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12617)

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

See Also

http://www.nessus.org/u?0d247a3f

https://svn.apache.org/viewvc?view=rev&rev=1809978

https://svn.apache.org/viewvc?view=rev&rev=1809992

https://svn.apache.org/viewvc?view=rev&rev=1810014

https://svn.apache.org/viewvc?view=rev&rev=1810026

Solution

Upgrade to Apache Tomcat version 7.0.82 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

EPSS Score

0.9436

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)

References

BID	100954
CVE	CVE-2017-12617
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CEA-ID:CEA-2019-0240

Exploitable With

Core Impact (true) (true) Metasploit (true)

Plugin Information

Published: 2017/10/11, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.82
```

124064 - Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.94. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.94_security-7 advisory.

- When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in- windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.m icrosoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong- way/). (CVE-2019-0232)

- The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

(CVE-2019-0221)

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

See Also

http://www.nessus.org/u?20cc80d0

http://www.nessus.org/u?3ba5edc6

http://www.nessus.org/u?41dddb4b

http://www.nessus.org/u?86be7b05

http://www.nessus.org/u?afa7a4e1

Solution

Upgrade to Apache Tomcat version 7.0.94 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.9422

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

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

References

BID	107906
CVE	CVE-2019-0221
CVE	CVE-2019-0232
XREF	CEA-ID:CEA-2021-0025

Exploitable With

Metasploit (true)

Plugin Information

Published: 2019/04/16, Modified: 2025/03/11

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.94
```

124064 - Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.94. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.94_security-7 advisory.

- When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in- windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.m icrosoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong- way/). (CVE-2019-0232)

- The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

(CVE-2019-0221)

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

See Also

http://www.nessus.org/u?20cc80d0

http://www.nessus.org/u?3ba5edc6

http://www.nessus.org/u?41dddb4b

http://www.nessus.org/u?86be7b05

http://www.nessus.org/u?afa7a4e1

Solution

Upgrade to Apache Tomcat version 7.0.94 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.9422

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

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

References

BID	107906
CVE	CVE-2019-0221
CVE	CVE-2019-0232
XREF	CEA-ID:CEA-2021-0025

Exploitable With

Metasploit (true)

Plugin Information

Published: 2019/04/16, Modified: 2025/03/11

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.94
```

197838 - Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.99. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.99_security-7 advisory.

- When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

- When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance. (CVE-2019-12418)

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

See Also

http://www.nessus.org/u?e1ae8f83

http://www.nessus.org/u?415f06c9

http://www.nessus.org/u?32c29167

Solution

Upgrade to Apache Tomcat version 7.0.99 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0243

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

CVE	CVE-2019-12418
CVE	CVE-2019-12418
CVE	CVE-2019-17563
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.99
```

197838 - Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.99. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.99_security-7 advisory.

- When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. (CVE-2019-17563)

- When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance. (CVE-2019-12418)

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

See Also

http://www.nessus.org/u?e1ae8f83

http://www.nessus.org/u?415f06c9

http://www.nessus.org/u?32c29167

Solution

Upgrade to Apache Tomcat version 7.0.99 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0243

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

CVE	CVE-2019-12418
CVE	CVE-2019-12418
CVE	CVE-2019-17563
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.99
```

197826 - Apache Tomcat 7.0.25 < 7.0.90

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.90. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.90_security-7 advisory.

- The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions Affected: Apache Tomcat 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, and 7.0.35 to 7.0.88. (CVE-2018-8034)

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://svn.apache.org/viewvc?view=rev&rev=1833760

http://www.nessus.org/u?45836195

Solution

Upgrade to Apache Tomcat version 7.0.90 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.2079

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

CVE	CVE-2018-8034

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.90
```

197826 - Apache Tomcat 7.0.25 < 7.0.90

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.90. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.90_security-7 advisory.

- The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions Affected: Apache Tomcat 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, and 7.0.35 to 7.0.88. (CVE-2018-8034)

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://svn.apache.org/viewvc?view=rev&rev=1833760

http://www.nessus.org/u?45836195

Solution

Upgrade to Apache Tomcat version 7.0.90 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.2079

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

CVE	CVE-2018-8034

Plugin Information

Published: 2024/05/23, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.90
```

138851 - Apache Tomcat 7.0.27 < 7.0.105

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.105. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.105_security-7 advisory.

- The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service. (CVE-2020-13935)

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

See Also

http://www.nessus.org/u?dd4dee09

http://www.nessus.org/u?81ec7286

http://www.nessus.org/u?58ae3a4f

Solution

Upgrade to Apache Tomcat version 7.0.105 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.9215

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

CVE	CVE-2020-13935
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/07/23, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.105
```

138851 - Apache Tomcat 7.0.27 < 7.0.105

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.105. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.105_security-7 advisory.

- The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service. (CVE-2020-13935)

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

See Also

http://www.nessus.org/u?dd4dee09

http://www.nessus.org/u?81ec7286

http://www.nessus.org/u?58ae3a4f

Solution

Upgrade to Apache Tomcat version 7.0.105 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.9215

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

CVE	CVE-2020-13935
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/07/23, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.105
```

121121 - Apache Tomcat 7.0.28 < 7.0.88

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.88. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.88_security-7 advisory.

- An improper handing of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the decoder causing a Denial of Service. Versions Affected: Apache Tomcat 9.0.0.M9 to 9.0.7, 8.5.0 to 8.5.30, 8.0.0.RC1 to 8.0.51, and 7.0.28 to 7.0.86. (CVE-2018-1336)

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

See Also

http://www.nessus.org/u?109a1a95

https://svn.apache.org/viewvc?view=rev&rev=1830376

Solution

Upgrade to Apache Tomcat version 7.0.88 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.15

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

CVE	CVE-2018-1336

Plugin Information

Published: 2019/01/11, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.88
```

121121 - Apache Tomcat 7.0.28 < 7.0.88

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.88. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.88_security-7 advisory.

- An improper handing of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the decoder causing a Denial of Service. Versions Affected: Apache Tomcat 9.0.0.M9 to 9.0.7, 8.5.0 to 8.5.30, 8.0.0.RC1 to 8.0.51, and 7.0.28 to 7.0.86. (CVE-2018-1336)

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

See Also

http://www.nessus.org/u?109a1a95

https://svn.apache.org/viewvc?view=rev&rev=1830376

Solution

Upgrade to Apache Tomcat version 7.0.88 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.15

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

CVE	CVE-2018-1336

Plugin Information

Published: 2019/01/11, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.88
```

17761 - OpenSSL 0.9.8 < 0.9.8i Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8i. It is, therefore, affected by a vulnerability as referenced in the 0.9.8i advisory.

- ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

(CVE-2009-1386)

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

See Also

http://www.nessus.org/u?f69832de

https://www.cve.org/CVERecord?id=CVE-2009-1386

Solution

Upgrade to OpenSSL version 0.9.8i or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.4763

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: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner            : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version     : 0.9.8i
```

17763 - OpenSSL 0.9.8 < 0.9.8k Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8k. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8k advisory.

- OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key. (CVE-2009-0789)

- The CMS_verify function in OpenSSL 0.9.8h through 0.9.8j, when CMS is enabled, does not properly handle errors associated with malformed signed attributes, which allows remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid. (CVE-2009-0591)

- The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length. (CVE-2009-0590)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2009-0590

https://www.cve.org/CVERecord?id=CVE-2009-0591

https://www.cve.org/CVERecord?id=CVE-2009-0789

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

Solution

Upgrade to OpenSSL version 0.9.8k or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.1292

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	34256
BID	73121
CVE	CVE-2009-0590
CVE	CVE-2009-0591
CVE	CVE-2009-0789

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8k
```

45359 - OpenSSL 0.9.8 < 0.9.8n Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8n. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8n advisory.

- The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information. (CVE-2010-0740)

- The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot. (CVE-2010-0433)

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

See Also

http://www.nessus.org/u?258ebd83

https://www.cve.org/CVERecord?id=CVE-2010-0433

https://www.cve.org/CVERecord?id=CVE-2010-0740

https://www.openssl.org/news/secadv/20100324.txt

Solution

Upgrade to OpenSSL version 0.9.8n or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.2191

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

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

References

BID	38533
BID	39013
CVE	CVE-2010-0433
CVE	CVE-2010-0740
XREF	Secunia:38807

Plugin Information

Published: 2010/03/26, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8n
```

200204 - OpenSSL 0.9.8 < 0.9.8q Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8q. It is, therefore, affected by a vulnerability as referenced in the 0.9.8q advisory.

- OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier. (CVE-2010-4180)

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://www.cve.org/CVERecord?id=CVE-2010-4180

https://www.openssl.org/news/secadv/20101202.txt

Solution

Upgrade to OpenSSL version 0.9.8q or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0589

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

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

STIG Severity

I

References

CVE	CVE-2010-4180
XREF	IAVA:2010-A-0167-S

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8q
```

58564 - OpenSSL 0.9.8 < 0.9.8u Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8u. It is, therefore, affected by a vulnerability as referenced in the 0.9.8u advisory.

- The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

(CVE-2012-0884)

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://www.cve.org/CVERecord?id=CVE-2012-0884

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

Solution

Upgrade to OpenSSL version 0.9.8u or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0335

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-2012-0884

Plugin Information

Published: 2012/04/02, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8u
```

59076 - OpenSSL 0.9.8 < 0.9.8x Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8x. It is, therefore, affected by a vulnerability as referenced in the 0.9.8x advisory.

- Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation. (CVE-2012-2333)

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

https://www.cve.org/CVERecord?id=CVE-2012-2333

Solution

Upgrade to OpenSSL version 0.9.8x or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.1324

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

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

References

BID	53476
CVE	CVE-2012-2333

Plugin Information

Published: 2012/05/11, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8x
```

64532 - OpenSSL 0.9.8 < 0.9.8y Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8y. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8y advisory.

- OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key. (CVE-2013-0166)

- The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the Lucky Thirteen issue. (CVE-2013-0169)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2013-0166

https://www.cve.org/CVERecord?id=CVE-2013-0169

https://www.openssl.org/news/secadv/20130205.txt

Solution

Upgrade to OpenSSL version 0.9.8y or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0415

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
XREF	CEA-ID:CEA-2019-0547

Plugin Information

Published: 2013/02/09, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8y
```

74363 - OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8za. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8za advisory.

- The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data. (CVE-2014-8176)

- Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow. (CVE-2015-0292)

- OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability. (CVE-2014-0224)

- The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake. (CVE-2014-0221)

- The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment. (CVE-2014-0195)

- The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

(CVE-2014-3470)

- The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack. (CVE-2014-0076)

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

See Also

https://www.openssl.org/news/secadv/20140605.txt

https://www.openssl.org/news/secadv/20150319.txt

https://www.openssl.org/news/secadv/20150611.txt

https://www.cve.org/CVERecord?id=CVE-2014-0076

https://www.cve.org/CVERecord?id=CVE-2014-0195

https://www.cve.org/CVERecord?id=CVE-2014-0221

https://www.cve.org/CVERecord?id=CVE-2014-0224

https://www.cve.org/CVERecord?id=CVE-2014-3470

https://www.cve.org/CVERecord?id=CVE-2014-8176

https://www.cve.org/CVERecord?id=CVE-2015-0292

Solution

Upgrade to OpenSSL version 0.9.8za or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.7

EPSS Score

0.9318

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	66363
BID	67898
BID	67899
BID	67900
BID	67901

CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
CVE	CVE-2014-8176
CVE	CVE-2015-0292
XREF	CERT:978508

Plugin Information

Published: 2014/06/06, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8za
```

77086 - OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zb. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8zb advisory.

- The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite. (CVE-2014-3510)

- The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

(CVE-2014-3508)

- Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function. (CVE-2014-3507)

- d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values. (CVE-2014-3506)

- Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition. (CVE-2014-3505)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2014-3505

https://www.cve.org/CVERecord?id=CVE-2014-3506

https://www.cve.org/CVERecord?id=CVE-2014-3507

https://www.cve.org/CVERecord?id=CVE-2014-3508

https://www.cve.org/CVERecord?id=CVE-2014-3510

https://www.openssl.org/news/secadv/20140806.txt

Solution

Upgrade to OpenSSL version 0.9.8zb or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.6603

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	69075
BID	69076
BID	69078
BID	69081
BID	69082
CVE	CVE-2014-3505
CVE	CVE-2014-3506
CVE	CVE-2014-3507
CVE	CVE-2014-3508
CVE	CVE-2014-3510

Plugin Information

Published: 2014/08/08, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8zb
```

82030 - OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zf. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8zf advisory.

- An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. (CVE-2016-0704)

- The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. (CVE-2016-0703)

- The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message. (CVE-2015-0293)

- The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c. (CVE-2015-0289)

- The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse. (CVE-2015-0287)

- The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature. (CVE-2015-0286)

- Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

(CVE-2015-0209)

- The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key. (CVE-2015-0288)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2015-0209

https://www.cve.org/CVERecord?id=CVE-2015-0286

https://www.cve.org/CVERecord?id=CVE-2015-0287

https://www.cve.org/CVERecord?id=CVE-2015-0288

https://www.cve.org/CVERecord?id=CVE-2015-0289

https://www.cve.org/CVERecord?id=CVE-2015-0293

https://www.cve.org/CVERecord?id=CVE-2016-0703

https://www.cve.org/CVERecord?id=CVE-2016-0704

https://www.openssl.org/news/secadv/20150319.txt

https://www.openssl.org/news/secadv/20160301.txt

Solution

Upgrade to OpenSSL version 0.9.8zf or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.2355

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

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

References

BID	73225
BID	73227
BID	73231
BID	73232
BID	73237
BID	73239
CVE	CVE-2015-0209
CVE	CVE-2015-0286
CVE	CVE-2015-0287
CVE	CVE-2015-0288
CVE	CVE-2015-0289
CVE	CVE-2015-0293
CVE	CVE-2016-0703
CVE	CVE-2016-0704

Plugin Information

Published: 2015/03/24, Modified: 2025/02/18

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8zf
```

84151 - OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zg. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8zg advisory.

- The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function. (CVE-2015-1792)

- The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data. (CVE-2015-1790)

- The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback. (CVE-2015-1789)

- Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier. (CVE-2015-1791)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2015-1789

https://www.cve.org/CVERecord?id=CVE-2015-1790

https://www.cve.org/CVERecord?id=CVE-2015-1791

https://www.cve.org/CVERecord?id=CVE-2015-1792

https://www.openssl.org/news/secadv/20150611.txt

Solution

Upgrade to OpenSSL version 0.9.8zg or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.1522

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

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

References

BID	75154
BID	75156
BID	75157
BID	75158
BID	75161
CVE	CVE-2015-1789
CVE	CVE-2015-1790
CVE	CVE-2015-1791
CVE	CVE-2015-1792

Plugin Information

Published: 2015/06/12, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner            : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version     : 0.9.8zg
```

17766 - OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow

Synopsis

The remote server is affected by a buffer overflow vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8p / 1.0.0b.

If a TLS server is multithreaded and uses the SSL cache, a remote attacker could trigger a buffer overflow and crash the server or run arbitrary code.

See Also

https://www.openssl.org/news/secadv/20101116.txt

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0b or later.

Risk Factor

High

VPR Score

5.9

EPSS Score

0.0736

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	44884
CVE	CVE-2010-3864

Plugin Information

Published: 2012/01/04, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8p
```

48205 - Apache 2.2.x < 2.2.16 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :

- A denial of service vulnerability in mod_cache and mod_dav. (CVE-2010-1452)

- An information disclosure vulnerability in mod_proxy_ajp, mod_reqtimeout, and mod_proxy_http relating to timeout conditions. Note that this issue only affects Apache on Windows, Netware, and OS/2. (CVE-2010-2068)

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

See Also

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

https://issues.apache.org/bugzilla/show_bug.cgi?id=49246

https://bz.apache.org/bugzilla/show_bug.cgi?id=49417

http://www.nessus.org/u?ce8ac446

Solution

Upgrade to Apache version 2.2.16 or later.

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)

VPR Score

3.6

EPSS Score

0.2372

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	40827
BID	41963
CVE	CVE-2010-1452
CVE	CVE-2010-2068
XREF	Secunia:40206

Plugin Information

Published: 2010/07/30, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.16
```

50070 - Apache 2.2.x < 2.2.17 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :

- Errors exist in the bundled expat library that may allow an attacker to crash the server when a buffer is over- read when parsing an XML document. (CVE-2009-3720 and CVE-2009-3560)

- An error exists in the 'apr_brigade_split_line' function in the bundled APR-util library. Carefully timed bytes in requests result in gradual memory increases leading to a denial of service. (CVE-2010-1623) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.17

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

Solution

Upgrade to Apache version 2.2.17 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.2511

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	37203
BID	36097
BID	43673
CVE	CVE-2009-3560
CVE	CVE-2009-3720
CVE	CVE-2010-1623
XREF	Secunia:41701
XREF	CWE:119

Plugin Information

Published: 2010/10/20, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.17
```

53896 - Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS

Synopsis

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

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr_fnmatch() function of the bundled APR library.

If mod_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.

Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.18

http://httpd.apache.org/security/vulnerabilities_22.html#2.2.18

http://securityreason.com/achievement_securityalert/98

Solution

Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.5553

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	47820
CVE	CVE-2011-0419
XREF	Secunia:44574

Plugin Information

Published: 2011/05/13, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.18
```

56216 - Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS

Synopsis

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

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod_proxy_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod_proxy_ajp' is used along with 'mod_proxy_balancer'.

Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.21

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

Solution

Upgrade to Apache version 2.2.21 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.3704

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	49616
CVE	CVE-2011-3348

Plugin Information

Published: 2011/09/16, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.21
```

57791 - Apache 2.2.x < 2.2.22 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :

- When configured as a reverse proxy, improper use of the RewriteRule and ProxyPassMatch directives could cause the web server to proxy requests to arbitrary hosts.

This could allow a remote attacker to indirectly send requests to intranet servers.

(CVE-2011-3368, CVE-2011-4317)

- A heap-based buffer overflow exists when mod_setenvif module is enabled and both a maliciously crafted 'SetEnvIf' directive and a maliciously crafted HTTP request header are used. (CVE-2011-3607)

- A format string handling error can allow the server to be crashed via maliciously crafted cookies.

(CVE-2012-0021)

- An error exists in 'scoreboard.c' that can allow local attackers to crash the server during shutdown.

(CVE-2012-0031)

- An error exists in 'protocol.c' that can allow 'HTTPOnly' cookies to be exposed to attackers through the malicious use of either long or malformed HTTP headers. (CVE-2012-0053)

- An error in the mod_proxy_ajp module when used to connect to a backend server that takes an overly long time to respond could lead to a temporary denial of service. (CVE-2012-4557)

Note that Nessus did not actually test for these flaws, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.22

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

Solution

Upgrade to Apache version 2.2.22 or later.

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

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

VPR Score

6.7

EPSS Score

0.8429

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

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

References

BID	49957
BID	50494
BID	50802
BID	51407
BID	51705
BID	51706
BID	56753
CVE	CVE-2011-3368
CVE	CVE-2011-3607
CVE	CVE-2011-4317
CVE	CVE-2012-0021
CVE	CVE-2012-0031
CVE	CVE-2012-0053
CVE	CVE-2012-4557

Plugin Information

Published: 2012/02/02, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.22
```

64912 - Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities

Synopsis

The remote web server is affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :

- Errors exist related to the modules mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp and unescaped hostnames and URIs that could allow cross- site scripting attacks. (CVE-2012-3499)

- An error exists related to the mod_proxy_balancer module's manager interface that could allow cross-site scripting attacks. (CVE-2012-4558)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.24

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

Solution

Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

EPSS Score

0.2823

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

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

References

BID	58165
CVE	CVE-2012-3499
CVE	CVE-2012-4558
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2013/02/27, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Installed version : 2.2.6
Fixed version     : 2.2.24
```

68915 - Apache 2.2.x < 2.2.25 Multiple Vulnerabilities

Synopsis

The remote web server may be affected by multiple cross-site scripting vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists in the 'RewriteLog' function where it fails to sanitize escape sequences from being written to log files, making it potentially vulnerable to arbitrary command execution. (CVE-2013-1862)

- A denial of service vulnerability exists relating to the 'mod_dav' module as it relates to MERGE requests. (CVE-2013-1896)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.25

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

http://www.nessus.org/u?f050c342

Solution

Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.4036

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	59826
BID	61129
CVE	CVE-2013-1862
CVE	CVE-2013-1896

Plugin Information

Published: 2013/07/16, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.25
```

73405 - Apache 2.2.x < 2.2.27 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :

- A flaw exists with the 'mod_dav' module that is caused when tracking the length of CDATA that has leading white space. A remote attacker with a specially crafted DAV WRITE request can cause the service to stop responding.
(CVE-2013-6438)

- A flaw exists in 'mod_log_config' module that is caused when logging a cookie that has an unassigned value. A remote attacker with a specially crafted request can cause the service to crash. (CVE-2014-0098)

Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner.

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2.27

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

Solution

Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.474

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	66303
CVE	CVE-2013-6438
CVE	CVE-2014-0098

Plugin Information

Published: 2014/04/08, Modified: 2018/09/17

Plugin Output

tcp/443/www

```
Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Installed version : 2.2.6
Fixed version     : 2.2.27
```

31118 - Apache 2.2.x < 2.2.8 Multiple Vulnerabilities (XSS, DoS)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.8. It is, therefore, affected by the following vulnerabilities :

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

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

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

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

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

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

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2

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

Solution

Upgrade to Apache version 2.2.8 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.8

EPSS Score

0.8687

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	26663
BID	26838
BID	27234
BID	27236
BID	27237
CVE	CVE-2007-5000
CVE	CVE-2007-6203
CVE	CVE-2007-6388
CVE	CVE-2007-6421
CVE	CVE-2007-6422
CVE	CVE-2008-0005
XREF	CWE:79
XREF	CWE:399

Plugin Information

Published: 2008/02/20, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.8
```

33477 - Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)

Synopsis

The remote web server may be affected by several issues.

Description

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.9. It is, therefore, affected by multiple vulnerabilities :

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

- A cross-site request forgery vulnerability in the balancer-manager interface of mod_proxy_balancer.

(CVE-2007-6420)

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

See Also

https://archive.apache.org/dist/httpd/CHANGES_2.2

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

Solution

Upgrade to Apache version 2.2.9 or later. Alternatively, ensure that the affected modules are not in use.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0504

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

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

References

BID	27236
BID	29653
CVE	CVE-2007-6420
CVE	CVE-2008-2364
CVE	CVE-2007-6423
XREF	Secunia:30621
XREF	CWE:352
XREF	CWE:399

Plugin Information

Published: 2008/07/11, Modified: 2018/06/29

Plugin Output

tcp/443/www

```
  Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Installed version : 2.2.6
  Fixed version     : 2.2.9
```

193420 - Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)

Synopsis

The remote web server is affected by an out-of-bound read vulnerability

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by an out-of-bounds read vulnerability as referenced in the 2.4.54 advisory.

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

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

See Also

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

Solution

Upgrade to Apache version 2.4.54 or later.

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)

VPR Score

1.4

EPSS Score

0.0019

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)

STIG Severity

I

References

CVE	CVE-2022-28330
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/443/www

```
URL               : https://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 2.2.6
Fixed version     : 2.4.54
```

17696 - 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)

VPR Score

3.3

EPSS Score

0.5039

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

tcp/443/www

```
Version source    : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Installed version : 2.2.6
Fixed version     : 2.2.8
```

88098 - 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)

VPR Score

5.9

EPSS Score

0.0032

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: 2025/02/11

Plugin Output

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: "24c22-2c-44adde00"
  Inode number           : 150562
  File size              : 44 bytes
  File modification time : Jul.  7, 2006 at 04:07:28 GMT
```

148405 - Apache Tomcat 7.0.0 < 7.0.107

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.107. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.107_security-7 advisory.

- When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances. (CVE-2021-24122)

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

See Also

http://www.nessus.org/u?f528c7ca

http://www.nessus.org/u?3e377be0

Solution

Upgrade to Apache Tomcat version 7.0.107 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.5394

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

CVE	CVE-2021-24122

Plugin Information

Published: 2021/04/09, Modified: 2025/03/13

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.107
```

148405 - Apache Tomcat 7.0.0 < 7.0.107

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.107. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.107_security-7 advisory.

- When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances. (CVE-2021-24122)

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

See Also

http://www.nessus.org/u?f528c7ca

http://www.nessus.org/u?3e377be0

Solution

Upgrade to Apache Tomcat version 7.0.107 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.5394

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

CVE	CVE-2021-24122

Plugin Information

Published: 2021/04/09, Modified: 2025/03/13

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.107
```

106975 - Apache Tomcat 7.0.0 < 7.0.85 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.85. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.85_security-7 advisory.

- Security constraints defined by annotations of Servlets in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 were only applied once a Servlet had been loaded. Because security constraints defined in this way apply to the URL pattern and any URLs below that point, it was possible - depending on the order Servlets were loaded - for some security constraints not to be applied.

This could have exposed resources to users who were not authorised to access them. (CVE-2018-1305)

- The URL pattern of (the empty string) which exactly maps to the context root was not correctly handled in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 when used as part of a security constraint definition. This caused the constraint to be ignored. It was, therefore, possible for unauthorised users to gain access to web application resources that should have been protected. Only security constraints with a URL pattern of the empty string were affected. (CVE-2018-1304)

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

See Also

http://www.nessus.org/u?df8da972

https://bz.apache.org/bugzilla/show_bug.cgi?id=62067

https://svn.apache.org/viewvc?view=rev&rev=1823309

https://svn.apache.org/viewvc?view=rev&rev=1823322

https://svn.apache.org/viewvc?view=rev&rev=1824360

Solution

Upgrade to Apache Tomcat version 7.0.85 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.1958

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

CVE	CVE-2018-1304
CVE	CVE-2018-1305

Plugin Information

Published: 2018/02/23, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.85
```

106975 - Apache Tomcat 7.0.0 < 7.0.85 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.85. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.85_security-7 advisory.

- Security constraints defined by annotations of Servlets in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 were only applied once a Servlet had been loaded. Because security constraints defined in this way apply to the URL pattern and any URLs below that point, it was possible - depending on the order Servlets were loaded - for some security constraints not to be applied.
This could have exposed resources to users who were not authorised to access them. (CVE-2018-1305)

- The URL pattern of (the empty string) which exactly maps to the context root was not correctly handled in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 when used as part of a security constraint definition. This caused the constraint to be ignored. It was, therefore, possible for unauthorised users to gain access to web application resources that should have been protected. Only security constraints with a URL pattern of the empty string were affected. (CVE-2018-1304)

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

See Also

http://www.nessus.org/u?df8da972

https://bz.apache.org/bugzilla/show_bug.cgi?id=62067

https://svn.apache.org/viewvc?view=rev&rev=1823309

https://svn.apache.org/viewvc?view=rev&rev=1823322

https://svn.apache.org/viewvc?view=rev&rev=1824360

Solution

Upgrade to Apache Tomcat version 7.0.85 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.1958

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

CVE	CVE-2018-1304
CVE	CVE-2018-1305

Plugin Information

Published: 2018/02/23, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.85
```

118035 - Apache Tomcat 7.0.23 < 7.0.91

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.91. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.91_security-7 advisory.

- When the default servlet in Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90 returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice. (CVE-2018-11784)

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

See Also

http://www.nessus.org/u?f0da50c8

https://svn.apache.org/viewvc?view=rev&rev=1840057

Solution

Upgrade to Apache Tomcat version 7.0.91 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.8512

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

CVE	CVE-2018-11784

Plugin Information

Published: 2018/10/10, Modified: 2024/05/23

Plugin Output

tcp/80/www

```

  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
  Installed version : 7.0.70
  Fixed version     : 7.0.91
```

118035 - Apache Tomcat 7.0.23 < 7.0.91

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.91. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.91_security-7 advisory.

- When the default servlet in Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90 returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice. (CVE-2018-11784)

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

See Also

http://www.nessus.org/u?f0da50c8

https://svn.apache.org/viewvc?view=rev&rev=1840057

Solution

Upgrade to Apache Tomcat version 7.0.91 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.8512

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

CVE	CVE-2018-11784

Plugin Information

Published: 2018/10/10, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```

  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Installed version : 7.0.70
  Fixed version     : 7.0.91
```

102587 - Apache Tomcat 7.0.41 < 7.0.79

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.79. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.79_security-7 advisory.

- The CORS Filter in Apache Tomcat 9.0.0.M1 to 9.0.0.M21, 8.5.0 to 8.5.15, 8.0.0.RC1 to 8.0.44 and 7.0.41 to 7.0.78 did not add an HTTP Vary header indicating that the response varies depending on Origin. This permitted client and server side cache poisoning in some circumstances. (CVE-2017-7674)

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

See Also

http://www.nessus.org/u?5c98678e

https://bz.apache.org/bugzilla/show_bug.cgi?id=61101

https://svn.apache.org/viewvc?view=rev&rev=1795816

Solution

Upgrade to Apache Tomcat version 7.0.79 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0539

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

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

References

BID	100280
CVE	CVE-2017-7674

Plugin Information

Published: 2017/08/18, Modified: 2024/05/23

Plugin Output

tcp/80/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Installed version : 7.0.70
Fixed version     : 7.0.79
```

102587 - Apache Tomcat 7.0.41 < 7.0.79

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.79. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.79_security-7 advisory.

- The CORS Filter in Apache Tomcat 9.0.0.M1 to 9.0.0.M21, 8.5.0 to 8.5.15, 8.0.0.RC1 to 8.0.44 and 7.0.41 to 7.0.78 did not add an HTTP Vary header indicating that the response varies depending on Origin. This permitted client and server side cache poisoning in some circumstances. (CVE-2017-7674)

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

See Also

http://www.nessus.org/u?5c98678e

https://bz.apache.org/bugzilla/show_bug.cgi?id=61101

https://svn.apache.org/viewvc?view=rev&rev=1795816

Solution

Upgrade to Apache Tomcat version 7.0.79 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0539

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

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

References

BID	100280
CVE	CVE-2017-7674

Plugin Information

Published: 2017/08/18, Modified: 2024/05/23

Plugin Output

tcp/8080/www

```
URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
Installed version : 7.0.70
Fixed version     : 7.0.79
```

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd

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

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

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: 2004/03/02, Modified: 2024/09/03

Plugin Output

tcp/80/www

```
The following default files were found :

http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd

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

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

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: 2004/03/02, Modified: 2024/09/03

Plugin Output

tcp/8080/www

```
The following default files were found :

http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. 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

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 v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Tue, 10 Feb 2026 12:40:23 GMT
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Access-Control-Allow-Origin: *
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
ETag: "24c22-2c-44adde00"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
```

```
Content-Type: text/html
<html><body><h1>It works!</h1></body></html>
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

11213 - 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

http://www.nessus.org/u?e979b5cb

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)

VPR Score

4.0

EPSS Score

0.6899

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: 2024/04/09

Plugin Output

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 : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus122140484.html HTTP/1.1
Connection: Close
Host: ec2-54-82-22-214.compute-1.amazonaws.com
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 ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.0 200 OK
Date: Tue, 10 Feb 2026 13:02:36 GMT
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Connection: close
Content-Type: message/http

TRACE /Nessus122140484.html HTTP/1.1
Connection: Close
Host: ec2-54-82-22-214.compute-1.amazonaws.com
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 ------------------------------\n
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

https://security.paloaltonetworks.com/PAN-SA-2020-0007

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.7

EPSS Score

0.323

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

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

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/80/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com/resources/js/
jquery-1.8.2.min.js
  Installed version : 1.8.2
  Fixed version     : 3.5.0
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

https://security.paloaltonetworks.com/PAN-SA-2020-0007

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.7

EPSS Score

0.323

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

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

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/8080/www

```
  URL               : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/resources/js/
jquery-1.8.2.min.js
  Installed version : 1.8.2
  Fixed version     : 3.5.0
```

17762 - OpenSSL 0.9.8 < 0.9.8j Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8j. It is, therefore, affected by a vulnerability as referenced in the 0.9.8j advisory.

- OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys. (CVE-2008-5077)

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://www.cve.org/CVERecord?id=CVE-2008-5077

https://www.openssl.org/news/secadv/20090107.txt

Solution

Upgrade to OpenSSL version 0.9.8j or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

EPSS Score

0.0107

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

Plugin Information

Published: 2012/01/04, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8j
```

80566 - OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zd. It is, therefore, affected by multiple vulnerabilities as referenced in the 0.9.8zd advisory.

- The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c. (CVE-2014-3570)

- The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the FREAK issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations. (CVE-2015-0204)

- OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.

(CVE-2014-8275)

- The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message. (CVE-2014-3572)

- OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c. (CVE-2014-3571)

- The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix. (CVE-2014-3569)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2014-3569

https://www.cve.org/CVERecord?id=CVE-2014-3570

https://www.cve.org/CVERecord?id=CVE-2014-3571

https://www.cve.org/CVERecord?id=CVE-2014-3572

https://www.cve.org/CVERecord?id=CVE-2014-8275

https://www.cve.org/CVERecord?id=CVE-2015-0204

https://www.openssl.org/news/secadv/20150108.txt

Solution

Upgrade to OpenSSL version 0.9.8zd or later.

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)

VPR Score

6.0

EPSS Score

0.9243

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	71934
BID	71935
BID	71936
BID	71937
BID	71939
BID	71942
CVE	CVE-2014-3569
CVE	CVE-2014-3570
CVE	CVE-2014-3571

CVE	CVE-2014-3572
CVE	CVE-2014-8275
CVE	CVE-2015-0204
XREF	CERT:243585

Plugin Information

Published: 2015/01/16, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Reported version : 0.9.8e
Fixed version    : 0.9.8zd
```

87219 - OpenSSL 0.9.8 < 0.9.8zh Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 0.9.8zh. It is, therefore, affected by a vulnerability as referenced in the 0.9.8zh advisory.

- The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application. (CVE-2015-3195)

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://www.cve.org/CVERecord?id=CVE-2015-3195

https://www.openssl.org/news/secadv/20151203.txt

Solution

Upgrade to OpenSSL version 0.9.8zh or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0204

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	78626
CVE	CVE-2015-3195

Plugin Information

Published: 2015/12/07, Modified: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8zh
```

17765 - 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

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

VPR Score

5.9

EPSS Score

0.0444

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: 2024/10/23

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8l
```

17767 - OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability

Synopsis

The remote SSL layer 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 0.9.8p / 1.0.0e.

A remote attacker could crash client software when using ECDH. The impact of this vulnerability is not clear; arbitrary code could be run too.

Note that OpenSSL changelog only reports a fix for 0.9.8p. 1.0.0a is definitely vulnerable. Gentoo reports a fix for 1.0.0e but it covers other flaws.NVD reports 0.9.7 as vulnerable too but does not give any fixed version.

See Also

https://www.mail-archive.com/openssl-dev@openssl.org/msg28049.html

Solution

Upgrade to OpenSSL 0.9.8p / 1.0.0e or later.

Risk Factor

Medium

VPR Score

4.2

EPSS Score

0.1413

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	42306

CVE	CVE-2010-2939
XREF	GLSA:201110-01

Plugin Information

Published: 2012/01/04, Modified: 2024/10/07

Plugin Output

tcp/443/www

```
  Banner           : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version : 0.9.8e
  Fixed version    : 0.9.8p
```

85582 - 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

tcp/80/www

```

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/index.html
```

85582 - 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

tcp/8080/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/index.html
```

34850 - Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in cleartext.

Description

The remote web server contains web pages that are protected by 'Basic'
authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution

Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:319
XREF	CWE:928
XREF	CWE:930
XREF	CWE:934

Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

Plugin Output

tcp/80/www

```
The following web pages use Basic Authentication over an unencrypted
channel :

/manager/html:/  realm="Tomcat Manager Application"
```

34850 - Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in cleartext.

Description

The remote web server contains web pages that are protected by 'Basic'
authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution

Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:319
XREF	CWE:928
XREF	CWE:930
XREF	CWE:934

Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

Plugin Output

tcp/8080/www

```
The following web pages use Basic Authentication over an unencrypted
channel :

/manager/html:/  realm="Tomcat Manager Application"
```

48204 - 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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2026/01/22

Plugin Output

tcp/443/www

```
URL        : https://ec2-54-82-22-214.compute-1.amazonaws.com/
Version    : 2.2.6
Source     : Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
backported : 0
modules    : mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
os         : Win32
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

NOTE: When paranoia levels are elevated, this plugin will also consider versions obtained from responses with non-200 HTTP status codes.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2026/01/22

Plugin Output

tcp/80/www

```
URL        : http://ec2-54-82-22-214.compute-1.amazonaws.com/
Version    : 7.0.70
backported : 0
source     : Apache Tomcat/7.0.70
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

NOTE: When paranoia levels are elevated, this plugin will also consider versions obtained from responses with non-200 HTTP status codes.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2026/01/22

Plugin Output

tcp/8080/www

```
  URL        : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  Version    : 7.0.70
  backported : 0
  source     : Apache Tomcat/7.0.70
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF	CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'searchTerm' parameter of the /search.html CGI :

/search.html?searchTerm=lypwsa

-------- output --------

<h2>Search Results:</h2>
No results were found for the query: lypwsa
</div>
</div>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)
```

```
http://ec2-54-82-22-214.compute-1.amazonaws.com/search.html?searchTerm=1ypwsa
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF	CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/8080/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'searchTerm' parameter of the /search.html CGI :

/search.html?searchTerm=lypwsa

-------- output --------

<h2>Search Results:</h2>
No results were found for the query: lypwsa
</div>
</div>
------------------------
```

33817 - 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: 2022/04/11

Plugin Output

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]

on site request forgery                   : S=1          SP=1         AP=1         SC=1         AC=1

SQL injection                             : S=112        SP=112       AP=280       SC=28
 AC=364
unseen parameters                         : S=140        SP=140       AP=350       SC=35
 AC=455
local file inclusion                      : S=16         SP=16        AP=40        SC=4         AC=52

web code injection                        : S=4          SP=4         AP=10        SC=1         AC=13

XML injection                             : S=4          SP=4         AP=10        SC=1         AC=13

format string                             : S=8          SP=8         AP=20        SC=2         AC=26

script injection                          : S=1          SP=1         AP=1         SC=1         AC=1

cross-site scripting (comprehensive test): S=68         SP=68        AP=170       SC=17
 AC=221
```

```
injectable parameter                     : S=8          SP=8         AP=20        SC=2         AC=26

cross-site scripting (extended patterns) : S=6          SP=6         AP=6         SC=6         AC=6

directory traversal (write access)       : S=8          SP=8         AP=20        SC=2         AC=26

SSI injection                            : S=12         SP=12        AP=30        SC=3         AC=39

header injection                         : S=2          SP=2         AP=2         SC=2         AC=2

HTML injection                           : S=5          SP=5         AP=5         SC=5         AC=5

directory traversal                      : S=116        SP=116       AP=290       SC=29
 AC=377
arbitrary command execution (time based) : S=24         SP=24        AP=60        SC=6         AC=78

persistent XSS                         [...]
```

33817 - 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: 2022/04/11

Plugin Output

tcp/8080/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]

SSI injection                             : S=12         SP=12         AP=30         SC=3          AC=39

arbitrary command execution (time based)  : S=24         SP=24         AP=60         SC=6          AC=78

cross-site scripting (comprehensive test): S=68         SP=68         AP=170        SC=17
 AC=221
HTTP response splitting                   : S=9          SP=9          AP=9          SC=9          AC=9

web code injection                        : S=4          SP=4          AP=10         SC=1          AC=13

format string                             : S=8          SP=8          AP=20         SC=2          AC=26

header injection                          : S=2          SP=2          AP=2          SC=2          AC=2

on site request forgery                   : S=1          SP=1          AP=1          SC=1          AC=1

SQL injection (2nd order)                 : S=4          SP=4          AP=10         SC=1          AC=13
```

```
directory traversal                      : S=116        SP=116       AP=290       SC=29
 AC=377
persistent XSS                           : S=16         SP=16        AP=40        SC=4         AC=52

blind SQL injection                      : S=48         SP=48        AP=120       SC=12
 AC=156
script injection                         : S=1          SP=1         AP=1         SC=1         AC=1

blind SQL injection (4 requests)         : S=16         SP=16        AP=40        SC=4         AC=52

XML injection                            : S=4          SP=4         AP=10        SC=1         AC=13

directory traversal (write access)       : S=8          SP=8         AP=20        SC=2         AC=26

arbitrary command execution              : S=88         SP=88        AP=220       SC=22
 AC=286
unseen parameters                      [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- SSI injection
- local file inclusion
- blind SQL injection (time based)
- blind SQL injection
- SQL injection (2nd order)
- web code injection
- SQL injection
- arbitrary command execution
- directory traversal
- directory traversal (extended test)
- cross-site scripting (comprehensive test)
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/8080/www

```
The following tests timed out without finding any flaw :
- cross-site scripting (comprehensive test)
- directory traversal (extended test)
- directory traversal
- blind SQL injection
- blind SQL injection (time based)
- local file inclusion
- SQL injection
- arbitrary command execution
```

49704 - 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

tcp/80/www

```

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


http://docs.oracle.com/javaee/6/api/index.html?javax/el/package-summary.html -
http://docs.oracle.com/javaee/6/api/index.html?javax/servlet/jsp/package-summary.html -
http://docs.oracle.com/javaee/6/api/index.html?javax/servlet/package-summary.html -
http://docs.oracle.com/javaee/7/api/javax/websocket/package-summary.html -
http://jcp.org/aboutJava/communityprocess/final/jsr315/index.html -
http://jcp.org/aboutJava/communityprocess/mrel/jsr245/index.html -
http://tomcat.apache.org/               -
http://tomcat.apache.org/connectors-doc/ -
http://tomcat.apache.org/connectors-doc/index.html -
http://tomcat.apache.org/findhelp.html  -
http://tomcat.apache.org/lists.html     -
http://wiki.apache.org/tomcat/FAQ       -
http://wiki.apache.org/tomcat/Specifications -
http://wiki.apache.org/tomcat/TomcatVersions -
http://www.apache.org/                  -
http://www.jcp.org                      -
https://jcp.org/aboutJava/communityprocess/mrel/jsr356/index.html -
https://www.microfocus.com/about/legal/#privacy -
```

49704 - 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

tcp/8080/www

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


http://docs.oracle.com/javaee/6/api/index.html?javax/el/package-summary.html - /docs/
http://docs.oracle.com/javaee/6/api/index.html?javax/servlet/jsp/package-summary.html - /docs/
http://docs.oracle.com/javaee/6/api/index.html?javax/servlet/package-summary.html - /docs/
http://docs.oracle.com/javaee/7/api/javax/websocket/package-summary.html - /docs/
http://jcp.org/aboutJava/communityprocess/final/jsr315/index.html - /docs/
http://jcp.org/aboutJava/communityprocess/mrel/jsr245/index.html - /docs/
http://tomcat.apache.org/               - /docs/
http://tomcat.apache.org/connectors-doc/ - /docs/
http://tomcat.apache.org/connectors-doc/index.html - /docs/
http://tomcat.apache.org/findhelp.html  - /docs/
http://tomcat.apache.org/lists.html     - /docs/
http://wiki.apache.org/tomcat/FAQ       - /docs/
http://wiki.apache.org/tomcat/Specifications - /docs/
http://wiki.apache.org/tomcat/TomcatVersions - /docs/
http://www.apache.org/                  - /docs/
http://www.jcp.org                      - /docs/
https://jcp.org/aboutJava/communityprocess/mrel/jsr356/index.html - /docs/
https://www.microfocus.com/about/legal/#privacy - /
```

84502 - 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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Tue, 10 Feb 2026 12:40:23 GMT
Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
Access-Control-Allow-Origin: *
Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
ETag: "24c22-2c-44adde00"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
<html><body><h1>It works!</h1></body></html>
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - 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: 2022/04/11

Plugin Output

tcp/80/www

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

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

    /
    /admin
    /resources
    /resources/css

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /docs
    /errors


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /backup
```

43111 - 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: 2022/04/11

Plugin Output

tcp/443/www

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

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

    /


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

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

    /

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
```

43111 - 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: 2022/04/11

Plugin Output

tcp/8080/www

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

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

    /
    /admin
    /resources
    /resources/css

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /docs
    /errors


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /backup
```

10107 - 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

tcp/80/www

```
The remote web server type is :

Apache-Coyote/1.1
```

10107 - 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

tcp/443/www

```
The remote web server type is :

Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
```

10107 - 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

tcp/8080/www

```
The remote web server type is :

Apache-Coyote/1.1
```

24260 - 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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 10 Feb 2026 16:43:09 GMT
  Server: Apache-Coyote/1.1
  Access-Control-Allow-Origin: *
  Cache-Control: no-cache, max-age=0, must-revalidate, no-store
  Content-Type: text/html;charset=UTF-8
  Content-Language: en
  Keep-Alive: timeout=5, max=98
  Connection: Keep-Alive
  Transfer-Encoding: chunked

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-
scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>
    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>
    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
                <div>
                 [...]
```

24260 - 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 is 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: 2024/02/26

Plugin Output

tcp/443/www

```

Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Tue, 10 Feb 2026 16:43:11 GMT
  Server: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Access-Control-Allow-Origin: *
  Last-Modified: Sat, 20 Nov 2004 14:16:24 GMT
  ETag: "24c22-2c-44adde00"
  Accept-Ranges: bytes
  Content-Length: 44
  Connection: close
  Content-Type: text/html

Response Body :

<html><body><h1>It works!</h1></body></html>
```

24260 - 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 is 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: 2024/02/26

Plugin Output

tcp/8080/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Cache-Control: no-cache, max-age=0, must-revalidate, no-store
  Content-Type: text/html;charset=UTF-8
  Content-Language: en
  Transfer-Encoding: chunked
  Date: Tue, 10 Feb 2026 16:42:56 GMT

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-
scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>
    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>
    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
            if (xhr.status == 403) {
                window.location.reload();
            }
        });
    </script>
</head>
<body>
    <div class="wrapper">
    <div class="navbar navbar-fixed-top">
        <div class="navbar-inner">
            <div class="container">
                <a href="/index.html" class="brand">Zero Bank</a>
                <div>
                    <ul class="nav float-right">
                        <li>    <form [...]
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80/www

```
  URL     : http://ec2-54-82-22-214.compute-1.amazonaws.com/resources/js/jquery-1.8.2.min.js
  Version : 1.8.2
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/8080/www

```
URL     : http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/resources/js/jquery-1.8.2.min.js
Version : 1.8.2
```

50344 - 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

tcp/80/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/index.html
```

50344 - 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

tcp/443/www

```

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

   - https://ec2-54-82-22-214.compute-1.amazonaws.com/
```

50344 - 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

tcp/8080/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/index.html
```

50345 - 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

tcp/80/www

```

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/index.html
```

50345 - 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

tcp/443/www

```

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

  - https://ec2-54-82-22-214.compute-1.amazonaws.com/
```

50345 - 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

tcp/8080/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/index.html
```

11219 - 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: 2025/07/14

Plugin Output

tcp/80/www

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

11219 - 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: 2025/07/14

Plugin Output

tcp/443/www

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

11219 - 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: 2025/07/14

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

19506 - 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: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.11.1
Nessus build : 20021
Plugin feed version : 202602092306
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Ethical non-intrusive scan of Zero Bank
Scan policy used : Web Application Tests
Scanner IP : 192.168.1.140
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 110.519 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : 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 : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/2/10 7:37 EST (UTC -05:00)
Scan duration : 18701 sec
Scan for malware : no
```

57323 - 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: 2026/01/22

Plugin Output

tcp/443/www

```
  Source              : Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40
  Reported version    : 0.9.8e
  Backported          : 0
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2026/01/13

Plugin Output

tcp/0

```

. You need to take the following 4 actions :

[ Apache 2.4.x < 2.4.59 Multiple Vulnerabilities (192923) ]

+ Action to take : Upgrade to Apache version 2.4.59 or later.

+Impact : Taking this action will resolve 75 different vulnerabilities (CVEs).


[ Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities (147163) ]

+ Action to take : Upgrade to Apache Tomcat version 7.0.108 or later.

+Impact : Taking this action will resolve 32 different vulnerabilities (CVEs).


[ JQuery 1.2 < 3.5.0 Multiple XSS (136929) ]

+ Action to take : Upgrade to JQuery version 3.5.0 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ OpenSSL 0.9.8 < 0.9.8zh Vulnerability (87219) ]

+ Action to take : Upgrade to OpenSSL version 0.9.8zh or later.

+Impact : Taking this action will resolve 63 different vulnerabilities (CVEs).
```

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/80/www

```
The following pages are protected by the Basic authentication scheme :

/manager/html
```

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/8080/www

```
The following pages are protected by the Basic authentication scheme :

/manager/html
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```

Potentially sensitive parameters for CGI /admin/currencies-add.html :

id : Potential horizontal or vertical privilege escalation

```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/8080/www

```

Potentially sensitive parameters for CGI /admin/currencies-add.html :

id : Potential horizontal or vertical privilege escalation

```

91815 - 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

tcp/80/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/errors/errors.log
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/resources/css/bootstrap.min.css
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/resources/css/font-awesome.css
  - http://ec2-54-82-22-214.compute-1.amazonaws.com/resources/css/main.css

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

91815 - 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

tcp/443/www

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

  - https://ec2-54-82-22-214.compute-1.amazonaws.com/

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

91815 - 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

tcp/8080/www

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

  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies-add.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/currencies.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/admin/users.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/docs/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/errors/
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/errors/errors.log
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/index.html
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/resources/css/bootstrap.min.css
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/resources/css/font-awesome.css
  - http://ec2-54-82-22-214.compute-1.amazonaws.com:8080/resources/css/main.css

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

11032 - 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: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/admin, /backup, /cgi-bin, /db, /htbin, /include, /stats, /testing, /docs, /errors, /scripts, /user

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

The following directories require authentication:
/manager/html
```

11032 - 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: 2024/06/07

Plugin Output

tcp/443/www

```
The following directories were discovered:
/cgi-bin

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
```

11032 - 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: 2024/06/07

Plugin Output

tcp/8080/www

```
The following directories were discovered:
/admin, /backup, /cgi-bin, /db, /htbin, /include, /stats, /testing, /docs, /errors, /scripts, /user

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

The following directories require authentication:
/manager/html
```

10662 - 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: 2026/01/26

Plugin Output

tcp/80/www

```

Webmirror performed 101 queries in 49s (2.061 queries per second)

The following CGIs have been discovered :


+ CGI : /search.html
  Methods : GET
  Argument : searchTerm


+ CGI : /admin/currencies-add.html
  Methods : POST
  Argument : country
  Argument : id
  Argument : name
```

10662 - 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: 2026/01/26

Plugin Output

tcp/8080/www

```

Webmirror performed 101 queries in 55s (1.0836 queries per second)

The following CGIs have been discovered :


+ CGI : /search.html
  Methods : GET
  Argument : searchTerm


+ CGI : /admin/currencies-add.html
  Methods : POST
  Argument : country
  Argument : id
  Argument : name
```