Windows expl 8080

Report generated by Tenable Nessus™ Sun, 29 Dec 2024 17:01:39 +04

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

111066 (1) - 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

0.1481

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

192.168.200.200 (tcp/8080/www)

```
URL              : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.89
```

171351 (1) - 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According to its version, Apache Tomcat is 7.0.x. It is, therefore, no longer maintained by its vendor or provider.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

192.168.200.200 (tcp/8080/www)

```
URL                                  : http://192.168.200.200:8080/
Installed version                    : 7.0.81
Security End of Life                 : March 31, 2021
Time since Security End of Life (Est.) : >= 3 years
```

197843 (1) - 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

9.0

EPSS Score

0.9742

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: 2024/05/24

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.100
```

103782 (1) - 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

9.2

EPSS Score

0.9733

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

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.82
```

121121 (1) - 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

0.0179

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

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.88
```

124064 (1) - 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

8.4

EPSS Score

0.9737

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: 2024/05/23

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.94
```

136770 (1) - 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

0.9319

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

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.104
```

138851 (1) - 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

0.4674

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

192.168.200.200 (tcp/8080/www)

```
URL              : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.105
```

147163 (1) - 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

0.0005

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

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.108
```

197826 (1) - 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

0.0056

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: 2024/05/23

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.90
```

197838 (1) - 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

0.0049

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: 2024/05/24

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.99
```

12085 (1) - 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

192.168.200.200 (tcp/8080/www)

```
The following default files were found :

http://192.168.200.200:8080/docs/
http://192.168.200.200:8080/examples/servlets/index.html
http://192.168.200.200:8080/examples/jsp/index.html
http://192.168.200.200:8080/examples/websocket/index.xhtml
```

```
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.
```

106710 (1) - Apache Tomcat 7.0.79 < 7.0.84

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.84. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.84_security-7 advisory.

- As part of the fix for bug 61201, the documentation for Apache Tomcat 9.0.0.M22 to 9.0.1, 8.5.16 to 8.5.23, 8.0.45 to 8.0.47 and 7.0.79 to 7.0.82 included an updated description of the search algorithm used by the CGI Servlet to identify which script to execute. The update was not correct. As a result, some scripts may have failed to execute as expected and other scripts may have been executed unexpectedly. Note that the behaviour of the CGI servlet has remained unchanged in this regard. It is only the documentation of the behaviour that was wrong and has been corrected. (CVE-2017-15706)

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?8cd0a415

https://bz.apache.org/bugzilla/show_bug.cgi?id=61201

https://svn.apache.org/viewvc?view=rev&rev=1814828

Solution

Upgrade to Apache Tomcat version 7.0.84 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:L/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0032

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-2017-15706

Plugin Information

Published: 2018/02/09, Modified: 2024/05/23

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.84
```

106975 (1) - 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

0.0048

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

192.168.200.200 (tcp/8080/www)

```
URL              : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.85
```

118035 (1) - 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

2.9

EPSS Score

0.892

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

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.91
```

148405 (1) - 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

0.0029

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: 2024/05/23

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL               : http://192.168.200.200:8080/
Installed version : 7.0.81
Fixed version     : 7.0.107
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.8939

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

192.168.200.200 (icmp/0)

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is 1 second.
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

192.168.200.200 (tcp/8080/www)

```
The remote web server type is :

Apache-Coyote/1.1
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

192.168.200.200 (udp/0)

```
For your information, here is the traceroute from 192.168.200.100 to 192.168.200.200 :
192.168.200.100
192.168.200.200

Hop Count: 1
```

11219 (1) - 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: 2024/05/20

Plugin Output

192.168.200.200 (tcp/8080/www)

```
Port 8080/tcp was found to be open
```

11422 (1) - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

192.168.200.200 (tcp/8080/www)

```
The default welcome page is from Tomcat.
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

192.168.200.200 (tcp/0)

```
Remote operating system : Microsoft Windows Server 2012 R2 Standard
Confidence level : 56
Method : MLSinFP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

HTTP:!:Server: Apache-Coyote/1.1

SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=8080


The remote host is running Microsoft Windows Server 2012 R2 Standard
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/10/04

Plugin Output

192.168.200.200 (tcp/0)

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202412290845
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1804-aarch64
Scan type : Normal
```

```
Scan name : Windows expl 8080
Scan policy used : Basic Network Scan
Scanner IP : 192.168.200.100
Port scanner(s) : nessus_syn_scanner
Port range : 8080
Ping RTT : 229.730 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 2
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
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 : 2024/12/29 16:59 +04
Scan duration : 106 sec
Scan for malware : no
```

20108 (1) - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

192.168.200.200 (tcp/8080/www)

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

22964 (1) - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

192.168.200.200 (tcp/8080/www)

```
A web server is running on this port.
```

24260 (1) - 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

192.168.200.200 (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
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Sun, 29 Dec 2024 13:00:10 GMT
  Connection: close

Response Body :

<!DOCTYPE html>
<html lang="en">
    <head>
        <title>Apache Tomcat/7.0.81</title>
        <link href="favicon.ico" rel="icon" type="image/x-icon" />
        <link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
        <link href="tomcat.css" rel="stylesheet" type="text/css" />
    </head>
```

```
    <body>
        <div id="wrapper">
            <div id="navigation" class="curved container">
                <span id="nav-home"><a href="http://tomcat.apache.org/">Home</a></span>
                <span id="nav-hosts"><a href="/docs/">Documentation</a></span>
                <span id="nav-config"><a href="/docs/config/">Configuration</a></span>
                <span id="nav-examples"><a href="/examples/">Examples</a></span>
                <span id="nav-wiki"><a href="http://wiki.apache.org/tomcat/FrontPage">Wiki</a></
span>
                <span id="nav-lists"><a href="http://tomcat.apache.org/lists.html">Mailing Lists</
a></span>
                <span id="nav-help"><a href="http://tomcat.apache.org/findhelp.html">Find Help</a></
span>
                <br class="separator" />
            </div>
            <div id="asf-box">
                <h1>Apache Tomcat/7.0.81</h1>
            </div>
            <div id="upper" class="curved container">
                <div id="congrats" class="curved container">
                    <h2>If you're seeing this, you've successfully installed Tomcat.
 Congratulations!</h2>
                </div>
                <div id="notice">
                    <img src="tomcat.png" alt="[tomcat logo]" />
                    <div id="tasks">
                        <h3> [...]
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

192.168.200.200 (tcp/0)

39446 (1) - 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.

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: 2024/11/14

Plugin Output

192.168.200.200 (tcp/8080/www)

```
URL        : http://192.168.200.200:8080/
Version    : 7.0.81
backported : 0
source     : Apache Tomcat/7.0.81
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/11/22

Plugin Output

192.168.200.200 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_server_2012:r2 -> Microsoft Windows Server 2012

Following application CPE matched on the remote system :

  cpe:/a:apache:tomcat:7.0.81 -> Apache Software Foundation Tomcat
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

192.168.200.200 (tcp/0)

```
Remote device type : unknown
Confidence level : 56
```

66334 (1) - 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: 2024/12/10

Plugin Output

192.168.200.200 (tcp/0)

```
. You need to take the following action :

[ 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 the following 11 different vulnerabilities :
CVE-2020-9484, CVE-2020-13935, CVE-2019-0232, CVE-2019-0221, CVE-2018-8014
CVE-2018-1336, CVE-2018-1305, CVE-2018-1304, CVE-2018-11784, CVE-2017-15706
CVE-2017-12617
```

86420 (1) - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

192.168.200.200 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 76:81:41:C0:F0:5F
```