test-scan(success-vitb)

Report generated by Nessus™ Wed, 18 Oct 2023 21:03:53 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

vtop.vitbhopal.ac.in

0	6	8	1	14
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Oct 18 20:48:50 2023
End time: Wed Oct 18 21:03:53 2023

Host Information

DNS Name: vtop.vitbhopal.ac.in
IP: 14.99.16.249

Vulnerabilities

166906 - Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability

Synopsis

The remote Apache Tomcat server is affected by a request smuggling vulnerability

Description

The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed_in_apache_tomcat_9.0.68_security-9 advisory. If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

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?0e8e4f33

http://www.nessus.org/u?ccba8e49

Solution

Upgrade to Apache Tomcat version 9.0.68 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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-42252
XREF	IAVA:2022-A-0457-S

Plugin Information

Published: 2022/11/03, Modified: 2023/04/18

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.68
```

138591 - Apache Tomcat 9.0.0.M1 < 9.0.37 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 9.0.37. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_9.0.37_security-9 advisory. 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?5733e550

http://www.nessus.org/u?d81c5cba

http://www.nessus.org/u?37703c60

Solution

Upgrade to Apache Tomcat version 9.0.37 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

5.1

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-2020-13934
CVE	CVE-2020-13935
XREF	IAVA:2020-A-0316-S
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/07/17, Modified: 2022/12/05

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.37
```

147164 - Apache Tomcat 9.0.0.M1 < 9.0.43 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 9.0.43. It is, therefore, affected by multiple vulnerabilities as referenced in the vendor 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)

- An information disclosure vulnerability exists when responding to new h2c connection requests, Apache Tomcat versions 9.0.0.M1 to 9.0.41 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request. (CVE-2021-25122)

- 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)

- A remote code execution vulnerability via deserialization exists when using Apache Tomcat 9.0.0.M1 to 9.0.41 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?00b2f5b4

http://www.nessus.org/u?c6d3f1a3

http://www.nessus.org/u?7051ce31

Solution

Upgrade to Apache Tomcat version 9.0.43 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

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

VPR Score

7.4

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)

STIG Severity

I

References

CVE	CVE-2020-9484
CVE	CVE-2021-25122
CVE	CVE-2021-25329
XREF	IAVA:2021-A-0114-S

XREF CEA-ID:CEA-2021-0004

Plugin Information

Published: 2021/03/05, Modified: 2022/12/05

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.43
```

171657 - Apache Tomcat 9.0.0.M1 < 9.0.71

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.71. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.71_security-9 advisory.

- Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.
(CVE-2023-24998)

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?4e5de685

http://www.nessus.org/u?47f6bf65

Solution

Upgrade to Apache Tomcat version 9.0.71 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

5.1

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-2023-24998
XREF	IAVA:2023-A-0112-S

Plugin Information

Published: 2023/02/20, Modified: 2023/03/27

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.71
```

160894 - Apache Tomcat 9.0.13 < 9.0.63 vulnerability

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.63. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.63_security-9 advisory.

- The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks. (CVE-2022-29885)

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?718f086d

http://www.nessus.org/u?1c4c7b12

Solution

Upgrade to Apache Tomcat version 9.0.63 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

5.1

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)

STIG Severity

III

References

CVE	CVE-2022-29885

XREF IAVA:2022-A-0222-S

Plugin Information

Published: 2022/05/10, Modified: 2023/04/07

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.63
```

144050 - Apache Tomcat 9.x < 9.0.40 Information Disclosure

Synopsis

The remote Apache Tomcat server is affected by an information disclosure vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.40. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_9.0.40_security-9 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)

- While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests. (CVE-2020-17527)

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?13c2f9e9

Solution

Upgrade to Apache Tomcat version 9.0.40 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

5.1

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-2020-17527
CVE	CVE-2021-24122
XREF	IAVA:2020-A-0570-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/10, Modified: 2022/12/05

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.40
```

151502 - Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_10.0.6_security-10 advisory.

- Queries made by the JNDI Realm did not always correctly escape parameters. Parameter values could be sourced from user provided data (eg user names) as well as configuration data provided by an administrator. In limited circumstances it was possible for users to authenticate using variations of their user name and/or to bypass some of the protection provided by the LockOut Realm. (CVE-2021-30640)

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?d3fb2d8e

http://www.nessus.org/u?0fb6f5ab

http://www.nessus.org/u?0d761c19

http://www.nessus.org/u?ddfa2b5e

http://www.nessus.org/u?95156892

http://www.nessus.org/u?ed08487c

http://www.nessus.org/u?806274b5

http://www.nessus.org/u?f104a57d

https://bz.apache.org/bugzilla/show_bug.cgi?id=65224

http://www.nessus.org/u?837a9443

Solution

Upgrade to Apache Tomcat version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-30640

Plugin Information

Published: 2021/07/12, Modified: 2023/06/20

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.46
```

141446 - Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This can lead to users seeing responses for unexpected resources.

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?0656cf04

http://www.nessus.org/u?771617a1

Solution

Upgrade to Apache Tomcat version 8.5.58, 9.0.38 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-13943
XREF	IAVA:2020-A-0465-S

Plugin Information

Published: 2020/10/14, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
  Installed version : 9.0.36
```

```
  Fixed version     : 9.0.38
```

152182 - Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.48. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.48_security-9 advisory.

- Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding;

and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.

(CVE-2021-33037)

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?3abdcc43

http://www.nessus.org/u?c2af8a80

http://www.nessus.org/u?d8db985a

http://www.nessus.org/u?19f14e83

Solution

Upgrade to Apache Tomcat version 9.0.48 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

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-2021-33037
XREF	IAVA:2021-A-0303-S

Plugin Information

Published: 2021/08/03, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.48
```

173251 - Apache Tomcat 9.0.0.M1 < 9.0.72

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.72. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.72_security-9 advisory.

- When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. (CVE-2023-28708)

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?f8ac9d8a

https://bz.apache.org/bugzilla/show_bug.cgi?id=66471

http://www.nessus.org/u?fa600361

Solution

Upgrade to Apache Tomcat version 9.0.72 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:L/I:N/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

1.4

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-2023-28708
XREF	IAVA:2023-A-0156-S

Plugin Information

Published: 2023/03/22, Modified: 2023/05/25

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.72
```

180194 - Apache Tomcat 9.0.0.M1 < 9.0.80

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.80. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.80_security-9 advisory.

- URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. The vulnerability is limited to the ROOT (default) web application. (CVE-2023-41080)

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?8401198b

http://www.nessus.org/u?b28e3588

Solution

Upgrade to Apache Tomcat version 9.0.80 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

3.8

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)

STIG Severity

I

References

CVE	CVE-2023-41080
XREF	IAVA:2023-A-0443-S

Plugin Information

Published: 2023/08/25, Modified: 2023/10/12

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.80
```

182809 - Apache Tomcat 9.0.0.M1 < 9.0.81 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 9.0.81. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_9.0.81_security-9 advisory.

- Tomcat did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. (CVE-2023-45648)

- Tomcat's HTTP/2 implementation was vulnerable to the rapid reset attack. The denial of service typically manifested as an OutOfMemoryError. (CVE-2023-44487)

- Tomcat's internal fork of a Commons FileUpload included an unreleased, in progress refactoring that exposed a potential denial of service on Windows if a web application opened a stream for an uploaded file but failed to close the stream. The file would never be deleted from disk creating the possibility of an eventual denial of service due to the disk being full. (CVE-2023-42794)

- When recycling various internal objects, including the request and the response, prior to re-use by the next request/response, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next. (CVE-2023-42795)

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?285c784f

http://www.nessus.org/u?ce3035d3

http://www.nessus.org/u?6e5b0c6b

http://www.nessus.org/u?da979f13

http://www.nessus.org/u?763fc1f5

Solution

Upgrade to Apache Tomcat version 9.0.81 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

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

VPR Score

7.7

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

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

STIG Severity

I

References

CVE	CVE-2023-42794
CVE	CVE-2023-42795
CVE	CVE-2023-44487
CVE	CVE-2023-45648
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	IAVA:2023-A-0534

Plugin Information

Published: 2023/10/10, Modified: 2023/10/17

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.81
```

162498 - Apache Tomcat 9.0.30 < 9.0.65 vulnerability

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 9.0.65. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_9.0.65_security-9 advisory.

- In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability. (CVE-2022-34305)

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?addecbc6

http://www.nessus.org/u?18afbeaa

Solution

Upgrade to Apache Tomcat version 9.0.65 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

4.6

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

II

References

CVE	CVE-2022-34305
XREF	IAVA:2022-A-0398-S

Plugin Information

Published: 2022/06/23, Modified: 2022/11/08

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.65
```

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: 2019/08/12

Plugin Output

tcp/443/www

```
The following default files were found :

https://vtop.vitbhopal.ac.in/docs/
https://vtop.vitbhopal.ac.in/examples/servlets/index.html
https://vtop.vitbhopal.ac.in/examples/jsp/index.html
https://vtop.vitbhopal.ac.in/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.
```

159464 - Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Apache Tomcat installed on the remote host is 9.x prior to 9.0.62.

- The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client. (CVE-2021-43980)

See Also

http://www.nessus.org/u?f8a02181

http://www.nessus.org/u?a9b73a07

Solution

Upgrade to Apache Tomcat version 9.0.62 or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

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

CVE CVE-2021-43980

Plugin Information

Published: 2022/04/01, Modified: 2023/03/21

Plugin Output

tcp/443/www

```
Installed version : 9.0.36
Fixed version     : 9.0.62
```

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.

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: 2023/05/24

Plugin Output

tcp/443/www

```
URL        : https://vtop.vitbhopal.ac.in/
Version    : 9.0.36
backported : 0
source     : Apache Tomcat/9.0.36
```

45590 - 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: 2023/10/16

Plugin Output

tcp/0

```
Following application CPE matched on the remote system :

  cpe:/a:apache:tomcat:9.0.36 -> Apache Software Foundation Tomcat
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
14.99.16.249 resolves as static-249.16.99.14-tataidc.co.in.
```

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: 2023/09/25

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: 2023/09/25

Plugin Output

tcp/443/www

```
Port 443/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310180342
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : test-scan2
Scan policy used : Advanced Scan
Scanner IP : 192.168.5.119
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 250.224 ms
Thorough tests : no
Experimental tests : 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 launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/18 20:49 India Standard Time
Scan duration : 891 sec
Scan for malware : no
```

50350 - OS Identification Failed

Synopsis

It was not possible to determine the remote operating system.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2020/01/22

Plugin Output

tcp/0

```
If you think these signatures would help us improve OS fingerprinting,
please send them to :

  os-signatures@nessus.org

Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.

SinFP:!:
```

```
P1:B10113:F0x12:W65535:O0204ffff:M1380:
P2:B10113:F0x12:W65535:O0204ffff0101040201030305:M1380:
P3:B00000:F0x00:W0:O0:M0
P4:190701_7_p=80R
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 443 was detected as being open but is now closed
```

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: 2023/10/10

Plugin Output

tcp/0

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

[ Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities (182809) ]

+ Action to take : Upgrade to Apache Tomcat version 9.0.81 or later.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).
```

22964 - 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: 2023/07/10

Plugin Output

tcp/80/www

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

22964 - 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: 2023/07/10

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

10287 - 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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.5.119 to 14.99.16.249 :
192.168.5.119

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
```

```
An error was detected along the way.

An error was detected along the way.
192.168.5.5
?
192.168.1.62
?
122.15.87.186
182.19.110.52
14.143.254.241
?
121.241.90.70
?
111.93.74.158
14.99.16.249

Hop Count: 16
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 302
rather than 404. The requested URL was :

    http://vtop.vitbhopal.ac.in/fvpI76W374F1.html
```