Scan Report

November 10, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "w2k8". The scan started at Mon Nov 10 01:14:39 2025 UTC and ended at Mon Nov 10 02:46:55 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.31	42	37	3	0	0
Total: 1	42	37	3	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 82 results selected by the filtering described above. Before filtering there were 196 results.

2 Results per Host

2.1 10.0.0.31

Host scan start	Mon Nov 10 01:15:05 2025 UTC
Host scan end	Mon Nov 10 02:46:49 2025 UTC

Service (Port)	Threat Level
8282/tcp	High
80/tcp	High
1617/tcp	High
3000/tcp	High
9200/tcp	High
8022/tcp	High
445/tcp	High
21/tcp	High
22/tcp	High
8282/tcp	Medium
4848/tcp	Medium
3000/tcp	Medium
9200/tcp	Medium
8022/tcp	Medium
135/tcp	Medium
21/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
22/tcp	Medium
9200/tcp	Low
general/tcp	Low
22/tcp	Low

2.1.1 High 8282/tcp

High (CVSS: 10.0)

NVT: Apache Axis2 Default Credentials (HTTP) - Active Check

Summary
The remote Apache Axis2 web interface is using known default credentials.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
```
It was possible to login at "http://10.0.0.31:8282/axis2/axis2-admin/" using the
↪ following credentials (Username:Password):
 - admin:axis2
```

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information, modify system configuration or execute code by uploading malicious webservices.

Solution:
Solution type: Mitigation
Change the password.

Vulnerability Insight
It was possible to login with default credentials: admin/axis2

Vulnerability Detection Method
Tries to login with default credentials via HTTP.
Details: `Apache Axis2 Default Credentials (HTTP) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.111006
Version used: `2023-10-19T05:05:21Z`

References
```
cve: CVE-2010-0219
url: https://www.exploit-db.com/exploits/15869
url: http://www.securityfocus.com/bid/44055
dfn-cert: DFN-CERT-2021-0775
```

High (CVSS: 10.0)

NVT: Apache Tomcat End of Life (EOL) Detection - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The "Apache Tomcat" version on the remote host has reached the end of life.
CPE: cpe:/a:apache:tomcat:8.0.33
Installed version: 8.0.33
Location/URL: 8282/tcp
EOL version: 8.0
EOL date: 2018-06-30

Impact
An EOL version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update the Apache Tomcat version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if an EOL version is present on the target host.
Details: Apache Tomcat End of Life (EOL) Detection - Windows
OID:1.3.6.1.4.1.25623.1.0.108134
Version used: 2025-04-15T05:54:49Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
url: https://tomcat.apache.org/tomcat-10.0-eol.html

. . . continues on next page . . .

... continued from previous page ...

```
url: https://tomcat.apache.org/tomcat-85-eol.html
url: https://tomcat.apache.org/tomcat-80-eol.html
url: https://tomcat.apache.org/tomcat-70-eol.html
url: https://tomcat.apache.org/tomcat-60-eol.html
url: https://tomcat.apache.org/tomcat-55-eol.html
url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases
url: https://tomcat.apache.org/whichversion.html
```

High (CVSS: 9.8)

NVT: Apache Tomcat RCE Vulnerability (Mar 2025) - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     9.0.99
Installation
path / port:       8282/tcp
```

Solution:

Solution type: VendorFix

Update to version 9.0.99, 10.1.35, 11.0.3 or later.

Affected Software/OS

Apache Tomcat version 9.0.98 and prior, 10.x through 10.1.34 and 11.0.0-M1 through 11.0.2.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight

The original implementation of partial PUT used a temporary file based on the user provided file name and path with the path separator replaced by '.'.
If all of the following are true, a malicious user is able to view security sensitive files and/or inject content into those files:

... continues on next page ...

... continued from previous page ...

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that is a sub-directory of a target URL for public uploads
- attacker knowledge of the names of security sensitive files being uploaded
- the security sensitive files also being uploaded via partial PUT

If all of the following are true, a malicious user is able to perform remote code execution:
- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- application is using Tomcat's file based session persistence with the default storage location
- application includes a library that may be leveraged in a deserialization attack

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat RCE Vulnerability (Mar 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.154161
Version used: `2025-04-11T15:45:04Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-24813`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.3`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.35`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.99`
`url: https://github.com/iSee857/CVE-2025-24813-PoC`
`url: https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is`
`↪-in-the-wild/`
`url: https://www.openwall.com/lists/oss-security/2025/03/10/5`
`url: https://scrapco.de/blog/analysis-of-cve-2025-24813-apache-tomcat-path-equiv`
`↪alence-rce.html`
`url: https://bishopfox.com/blog/tomcat-cve-2025-24813-what-you-need-to-know-blog`
`cert-bund: WID-SEC-2025-1564`
`cert-bund: WID-SEC-2025-1439`
`cert-bund: WID-SEC-2025-0825`
`cert-bund: WID-SEC-2025-0824`
`cert-bund: WID-SEC-2025-0823`
`cert-bund: WID-SEC-2025-0511`
`dfn-cert: DFN-CERT-2025-2098`
`dfn-cert: DFN-CERT-2025-0993`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2025-0890
dfn-cert: DFN-CERT-2025-0888
dfn-cert: DFN-CERT-2025-0766
dfn-cert: DFN-CERT-2025-0622

High (CVSS: 9.8)

NVT: Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a rewrite rule bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 9.0.104
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 9.0.104, 10.1.40, 11.0.6 or later.

Affected Software/OS
Apache Tomcat version 9.0.102 and prior, 10.x through 10.1.39 and 11.0.0-M1 through 11.0.5.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
For a subset of unlikely rewrite rule configurations, it is possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.154400
Version used: 2025-05-06T05:40:10Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2025-31651
url: https://lists.apache.org/thread/cpklvqwvdrp4k9hmd2l3q33j0gzy4fox
cert-bund: WID-SEC-2025-2372
cert-bund: WID-SEC-2025-1850
cert-bund: WID-SEC-2025-1572
cert-bund: WID-SEC-2025-1565
cert-bund: WID-SEC-2025-1563
cert-bund: WID-SEC-2025-1439
cert-bund: WID-SEC-2025-1365
cert-bund: WID-SEC-2025-0895
dfn-cert: DFN-CERT-2025-2285
dfn-cert: DFN-CERT-2025-2098
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1905
dfn-cert: DFN-CERT-2025-1898
dfn-cert: DFN-CERT-2025-1557
dfn-cert: DFN-CERT-2025-1081

High (CVSS: 9.1)

NVT: Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.37

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        8282/tcp
```

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information and bypass certain security restrictions.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.0.M10 or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, Apache Tomcat versions 8.5.0 to 8.5.4, Apache Tomcat versions 8.0.0.RC1 to 8.0.36, Apache Tomcat versions 7.0.0 to 7.0.70, and Apache Tomcat versions 6.0.0 to 6.0.45 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- An error in the system property replacement feature for configuration files.
- An error in the realm implementations in Apache Tomcat that does not process the supplied password if the supplied user name did not exist.
- An error in the configured SecurityManager via a Tomcat utility method that is accessible to web applications.
- An error in the configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.
- An error in the ResourceLinkFactory implementation in Apache Tomcat that does not limit web application access to global JNDI resources to those resources explicitly linked to the web application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Wind.` ↪..
OID:1.3.6.1.4.1.25623.1.0.811298
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2016-6794`
`cve: CVE-2016-0762`
`cve: CVE-2016-5018`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-6796
cve: CVE-2016-6797
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72
url: http://www.securityfocus.com/bid/93940
url: http://www.securityfocus.com/bid/93944
url: http://www.securityfocus.com/bid/93939
url: http://www.securityfocus.com/bid/93942
url: http://www.securityfocus.com/bid/93943
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8
↪.0.37
cert-bund: WID-SEC-2022-1910
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/1031
cert-bund: CB-K17/0659
cert-bund: CB-K17/0397
cert-bund: CB-K17/0133
cert-bund: CB-K16/1927
cert-bund: CB-K16/1673
cert-bund: CB-K16/1646
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-1064
dfn-cert: DFN-CERT-2017-0673
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2016-2035
dfn-cert: DFN-CERT-2016-1772
dfn-cert: DFN-CERT-2016-1743
```

High (CVSS: 9.1)

NVT: Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 8.0.42`
`Installation path / port: 8282/tcp`

Impact
Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:
Solution type: VendorFix
Upgrade to version 9.0.0.M18, 8.5.12, 8.0.42, 7.0.76 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M17,
Apache Tomcat versions 8.5.0 to 8.5.11,
Apache Tomcat versions 8.0.0.RC1 to 8.0.41 and
Apache Tomcat versions 7.0.0 to 7.0.75 on Windows

Vulnerability Insight
A some calls to application listeners 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.810764
Version used: `2024-02-15T05:05:40Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2017-5648`
`url: http://tomcat.apache.org/security-9.html`
`url: http://tomcat.apache.org/security-8.html`
`url: http://tomcat.apache.org/security-7.html`
`url: http://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882b`

... continues on next page ...

... continued from previous page ...

```
↪f6860397368a52600@%3Cannounce.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0047
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/1060
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624
```

High (CVSS: 7.8)

NVT: Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     9.0.107
Installation
path / port:       8282/tcp
```

Solution:

Solution type: VendorFix

Update to version 9.0.107, 10.1.43, 11.0.9 or later.

Affected Software/OS

Apache Tomcat version 9.0.106 and prior, 10.x through 10.1.42 and 11.0.0-M1 through 11.0.8.

... continues on next page ...

... continued from previous page ...

Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
The following flaws exist:
- CVE-2025-52520: DoS due to overflow in file upload limit
- CVE-2025-53506: DoS via excessive HTTP/2 streams

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.154896
Version used: `2025-07-11T15:43:14Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-52520`
`cve: CVE-2025-53506`
`url: https://lists.apache.org/thread/trqq01bbxw6c92zx69kx2mw2qgmfy0o5`
`url: https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.43`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.9`
`cert-bund: WID-SEC-2025-1905`
`cert-bund: WID-SEC-2025-1468`
`dfn-cert: DFN-CERT-2025-2390`
`dfn-cert: DFN-CERT-2025-2335`
`dfn-cert: DFN-CERT-2025-2299`
`dfn-cert: DFN-CERT-2025-2219`
`dfn-cert: DFN-CERT-2025-2168`
`dfn-cert: DFN-CERT-2025-2088`
`dfn-cert: DFN-CERT-2025-2056`
`dfn-cert: DFN-CERT-2025-1991`
`dfn-cert: DFN-CERT-2025-1789`

High (CVSS: 7.8)

NVT: Apache Tomcat DoS Vulnerability (Jul 2024) - Windows

Product detection result
`cpe:/a:apache:tomcat:8.0.33`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`
`↪7652)`

Summary
Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 9.0.90`
`Installation`
`path / port: 8282/tcp`

Solution:
Solution type: VendorFix
Update to version 9.0.90, 10.1.25, 11.0.0-M21 or later.

Affected Software/OS
Apache Tomcat versions prior to 9.0.90, 10.x through 10.1.24 and 11.0.0-M1 through 11.0.0-M20. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat DoS Vulnerability (Jul 2024) - Windows`
OID:1.3.6.1.4.1.25623.1.0.152544
Version used: `2024-12-19T05:05:34Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`

. . . continues on next page . . .

... continued from previous page ...

Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2024-34750
url: https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l
url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M2
↪1
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.25
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.90
cert-bund: WID-SEC-2025-0163
cert-bund: WID-SEC-2025-0161
cert-bund: WID-SEC-2025-0148
cert-bund: WID-SEC-2025-0144
cert-bund: WID-SEC-2025-0143
cert-bund: WID-SEC-2024-3197
cert-bund: WID-SEC-2024-3195
cert-bund: WID-SEC-2024-2100
cert-bund: WID-SEC-2024-1905
cert-bund: WID-SEC-2024-1522
dfn-cert: DFN-CERT-2025-2098
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1517
dfn-cert: DFN-CERT-2025-0170
dfn-cert: DFN-CERT-2025-0146
dfn-cert: DFN-CERT-2024-2192
dfn-cert: DFN-CERT-2024-2031
dfn-cert: DFN-CERT-2024-1723

High (CVSS: 7.8)

NVT: Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary

Apache Tomcat is prone to a session fixation vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 8.0.33
Fixed version:     9.0.106
Installation
path / port:       8282/tcp
```

Solution:
Solution type: VendorFix
Update to version 9.0.106, 10.1.42, 11.0.8 or later.

Affected Software/OS
Apache Tomcat versions prior to 9.0.106, 10.1.0-M1 through 10.1.41 and 11.0.0-M1 through 11.0.7.

Vulnerability Insight
If the rewrite valve was enabled for a web application, an attacker was able to craft a URL that, if a victim clicked on it, would cause the victim's interaction with that resource to occur in the context of the attacker's session.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.127943
Version used: `2025-08-21T05:40:06Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-55668`
`url: https://lists.apache.org/thread/v6bknr96rl7l1qxkl1c03v0qdvbbqs47`
`cert-bund: WID-SEC-2025-1905`
`cert-bund: WID-SEC-2025-1826`
`dfn-cert: DFN-CERT-2025-1588`

High (CVSS: 7.8)

NVT: Apache Tomcat DoS Vulnerability (Jul 2025) - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

... continues on next page ...

... continued from previous page ...

Summary
Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 9.0.107`
`Installation path / port: 8282/tcp`

Solution:
Solution type: VendorFix
Update to version 9.0.107 or later.

Affected Software/OS
Apache Tomcat version 9.0.106 and prior.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
A race condition on connection close could trigger a JVM crash when using the APR/Native connector leading to a DoS. This was particularly noticeable with client initiated closes of HTTP/2 connections.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat DoS Vulnerability (Jul 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.154918
Version used: `2025-07-11T15:43:14Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-52434`
`url: https://lists.apache.org/thread/gxgh65004f25y8519coth6w7vchww030`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107`
`cert-bund: WID-SEC-2025-1905`
`cert-bund: WID-SEC-2025-1468`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2025-2957
dfn-cert: DFN-CERT-2025-2390
dfn-cert: DFN-CERT-2025-2299
dfn-cert: DFN-CERT-2025-2056
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1789

High (CVSS: 7.8)

NVT: Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to is prone to a denial of service (DoS) vulnerability in the HTTP/2 protocol dubbed 'MadeYouReset'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 9.0.108
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 9.0.108, 10.1.44, 11.0.10 or later.

Affected Software/OS
Apache Tomcat version 9.0.107 and prior, 10.x through 10.1.43 and 11.0.0-M1 through 11.0.9.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

A mismatch caused by client-triggered server-sent stream resets between HTTP/2 specifications and the internal architectures of some HTTP/2 implementations may result in excessive server resource consumption leading to denial-of-service (DoS). By opening streams and then rapidly triggering the server to reset them, using malformed frames or flow control errors, an attacker can exploit incorrect stream accounting. Streams reset by the server are considered closed at the protocol level, even though backend processing continues. This allows a client to cause the server to handle an unbounded number of concurrent streams on a single connection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows`
OID:1.3.6.1.4.1.25623.1.0.171673
Version used: `2025-08-26T05:39:52Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-8671`
`cve: CVE-2025-48989`
`url: https://lists.apache.org/thread/9ydfg0xr0tchmglcprhxgwhj0hfwxlyf`
`url: https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.108`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.44`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.10`
`url: https://galbarnahum.com/posts/made-you-reset-intro`
`url: https://deepness-lab.org/publications/madeyoureset/`
`url: https://kb.cert.org/vuls/id/767506`
`url: https://thehackernews.com/2025/08/new-http2-madeyoureset-vulnerability.html`
`cert-bund: WID-SEC-2025-2373`
`cert-bund: WID-SEC-2025-2361`
`cert-bund: WID-SEC-2025-2360`
`cert-bund: WID-SEC-2025-2357`
`cert-bund: WID-SEC-2025-2356`
`cert-bund: WID-SEC-2025-1830`
`dfn-cert: DFN-CERT-2025-2957`
`dfn-cert: DFN-CERT-2025-2390`
`dfn-cert: DFN-CERT-2025-2299`
`dfn-cert: DFN-CERT-2025-2224`
`dfn-cert: DFN-CERT-2025-2219`

High (CVSS: 7.8)

NVT: Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows

Product detection result
`cpe:/a:apache:tomcat:8.0.33`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`
`↪7652)`

Summary
Apache Tomcat is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 9.0.106`
`Installation`
`path / port: 8282/tcp`

Solution:
Solution type: VendorFix
Update to version 9.0.106, 10.1.42, 11.0.8 or later.

Affected Software/OS
Apache Tomcat version 9.0.105 and prior, 10.x through 10.1.41 and 11.0.0-M1 through 11.0.7.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
The following flaws exist:
- CVE-2025-48976: Denial of service (DoS) in Apache Commons FileUpload
- CVE-2025-48988: DoS in multipart upload
- CVE-2025-49125: Security constraint bypass for pre/post-resources

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.154755
Version used: `2025-06-24T05:41:22Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`

. . . continues on next page . . .

... continued from previous page ...

Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2025-48976
cve: CVE-2025-48988
cve: CVE-2025-49125
url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.8
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.42
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.106
url: https://lists.apache.org/thread/nzkqsok8t42qofgqfmck536mtyzygp18
url: https://lists.apache.org/thread/m66cytbfrty9k7dc4cg6tl1czhsnbywk
url: https://www.openwall.com/lists/oss-security/2025/06/16/1
url: https://www.openwall.com/lists/oss-security/2025/06/16/2
url: https://github.com/Samb102/POC-CVE-2025-48988-CVE-2025-48976
cert-bund: WID-SEC-2025-2373
cert-bund: WID-SEC-2025-2372
cert-bund: WID-SEC-2025-2371
cert-bund: WID-SEC-2025-2369
cert-bund: WID-SEC-2025-2366
cert-bund: WID-SEC-2025-2362
cert-bund: WID-SEC-2025-2361
cert-bund: WID-SEC-2025-2360
cert-bund: WID-SEC-2025-2359
cert-bund: WID-SEC-2025-2357
cert-bund: WID-SEC-2025-2356
cert-bund: WID-SEC-2025-2355
cert-bund: WID-SEC-2025-2353
cert-bund: WID-SEC-2025-2351
cert-bund: WID-SEC-2025-1562
cert-bund: WID-SEC-2025-1560
cert-bund: WID-SEC-2025-1559
cert-bund: WID-SEC-2025-1335
cert-bund: WID-SEC-2025-1334
dfn-cert: DFN-CERT-2025-2941
dfn-cert: DFN-CERT-2025-2939
dfn-cert: DFN-CERT-2025-2390
dfn-cert: DFN-CERT-2025-2335
dfn-cert: DFN-CERT-2025-2299
dfn-cert: DFN-CERT-2025-2291
dfn-cert: DFN-CERT-2025-2098
dfn-cert: DFN-CERT-2025-2088
dfn-cert: DFN-CERT-2025-2056
dfn-cert: DFN-CERT-2025-1992
dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1780

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2025-1739
dfn-cert: DFN-CERT-2025-1588

High (CVSS: 7.5)

NVT: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.41
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow remote attackers to gain access to potentially sensitive information.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M13, Apache Tomcat versions 8.5.0 to 8.5.8, Apache Tomcat versions 8.0.0.RC1 to 8.0.39, Apache Tomcat versions 7.0.0 to 7.0.73, and Apache Tomcat versions 6.0.16 to 6.0.48 on Windows.

Vulnerability Insight
The flaw exists due to error handling of the send file code for the NIO HTTP connector in Apache Tomcat resulting in the current Processor object being added to the Processor cache multiple times. This in turn means 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.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.811296
Version used: 2024-02-15T05:05:40Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2016-8745
url: https://bz.apache.org/bugzilla/show_bug.cgi?id=60409
url: http://www.securityfocus.com/bid/94828
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41
url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9
url: http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0303
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1929
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0308
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-2037

High (CVSS: 7.5)

NVT: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.43
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:
Solution type: VendorFix
Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M18, Apache Tomcat versions 8.5.0 to 8.5.12, Apache Tomcat versions 8.0.0.RC1 to 8.0.42, Apache Tomcat versions 7.0.0 to 7.0.76 and Apache Tomcat versions 6.0.0 to 6.0.52 on Windows.

Vulnerability Insight
A bug in the handling of the pipelined requests when send file was used resulted in the pipelined request being lost when send file processing of the previous request completed.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability - Windo.
↪..
OID:1.3.6.1.4.1.25623.1.0.810762
Version used: 2024-02-15T05:05:40Z

Product Detection Result
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2017-5647
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: http://tomcat.apache.org/security-6.html
url: https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0
↪dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0047
cert-bund: CB-K17/1831
cert-bund: CB-K17/1423
cert-bund: CB-K17/1246
cert-bund: CB-K17/1205
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0801
cert-bund: CB-K17/0604
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1485
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1243
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0828
dfn-cert: DFN-CERT-2017-0624

High (CVSS: 7.5)

NVT: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows

Product detection result

cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary

Apache Tomcat is prone to a denial of service (DoS) vulnerability.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.5.85
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 8.5.85, 9.0.71, 10.1.5, 11.0.0-M3 or later.

Affected Software/OS
Apache Tomcat versions through 8.5.84, 9.0.0-M1 through 9.0.70, 10.x through 10.1.4 and 11.0.0-M1 only.

Vulnerability Insight
Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat DoS Vulnerability (Feb 2023) - Windows
OID:1.3.6.1.4.1.25623.1.0.104551
Version used: 2025-01-21T05:37:33Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2023-24998
url: https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1
url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85
url: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy
cert-bund: WID-SEC-2025-0810
cert-bund: WID-SEC-2024-1652
cert-bund: WID-SEC-2024-1642

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-1637
cert-bund: WID-SEC-2024-1622
cert-bund: WID-SEC-2024-1238
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0888
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2024-0117
cert-bund: WID-SEC-2024-0054
cert-bund: WID-SEC-2023-2688
cert-bund: WID-SEC-2023-2675
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2309
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1817
cert-bund: WID-SEC-2023-1815
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1811
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1808
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1792
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1782
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1142
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-1012
cert-bund: WID-SEC-2023-1007
cert-bund: WID-SEC-2023-1005
cert-bund: WID-SEC-2023-0609
cert-bund: WID-SEC-2023-0433
dfn-cert: DFN-CERT-2025-1992
dfn-cert: DFN-CERT-2024-2151
dfn-cert: DFN-CERT-2024-1865
dfn-cert: DFN-CERT-2024-1006
dfn-cert: DFN-CERT-2024-0059
dfn-cert: DFN-CERT-2024-0048
dfn-cert: DFN-CERT-2023-2778
dfn-cert: DFN-CERT-2023-2545

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2054
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1362
dfn-cert: DFN-CERT-2023-1109
dfn-cert: DFN-CERT-2023-0902
dfn-cert: DFN-CERT-2023-0886
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0763
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2023-0540
dfn-cert: DFN-CERT-2023-0414

High (CVSS: 7.5)

NVT: Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.53
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Apache Tomcat versions 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 on Windows.

Vulnerability Insight
The flaw exists due to a missing host name verification when using TLS with the WebSocket client.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813742
Version used: `2025-09-17T05:39:26Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2018-8034`
`url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201`
`↪80722091057.GA70283@minotaur.apache.org%3E`
`url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53`
`url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32`
`url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90`
`cert-bund: WID-SEC-2024-1682`
`cert-bund: WID-SEC-2024-0528`
`cert-bund: CB-K19/0907`
`cert-bund: CB-K19/0616`
`cert-bund: CB-K19/0320`
`cert-bund: CB-K18/1005`
`cert-bund: CB-K18/0809`
`dfn-cert: DFN-CERT-2019-2418`
`dfn-cert: DFN-CERT-2019-1627`
`dfn-cert: DFN-CERT-2019-1237`
`dfn-cert: DFN-CERT-2019-0951`
`dfn-cert: DFN-CERT-2019-0451`
`dfn-cert: DFN-CERT-2019-0147`
`dfn-cert: DFN-CERT-2018-2165`
`dfn-cert: DFN-CERT-2018-2142`
`dfn-cert: DFN-CERT-2018-1753`
`dfn-cert: DFN-CERT-2018-1471`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2018-1443
dfn-cert: DFN-CERT-2018-1262

High (CVSS: 7.5)

NVT: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.36
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial of service (CPU consumption).

Solution:
Solution type: VendorFix
Upgrade to version 7.0.70, or 8.0.36, or 8.5.3, or 9.0.0.M7, or later.

Affected Software/OS
Apache Tomcat 7.x before 7.0.70, 8.0.0.RC1 before 8.0.36, 8.5.x before 8.5.3, and 9.0.0.M1 before 9.0.0.M7.

Vulnerability Insight
The flaw is due to an error in the 'MultipartStream' class in Apache Commons Fileupload when processing multi-part requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'MultipartStream' Class DoS Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.808197

... continues on next page ...

... continued from previous page ...

Version used: 2022-04-13T13:17:10Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2016-3092
url: http://tomcat.apache.org/security-7.html
url: http://www.securityfocus.com/bid/91453
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-9.html
cert-bund: WID-SEC-2023-0644
cert-bund: WID-SEC-2022-1537
cert-bund: WID-SEC-2022-1375
cert-bund: CB-K18/0605
cert-bund: CB-K17/1750
cert-bund: CB-K17/1198
cert-bund: CB-K17/1060
cert-bund: CB-K17/0657
cert-bund: CB-K17/0397
cert-bund: CB-K16/1993
cert-bund: CB-K16/1799
cert-bund: CB-K16/1758
cert-bund: CB-K16/1322
cert-bund: CB-K16/1002
cert-bund: CB-K16/0993
dfn-cert: DFN-CERT-2023-0574
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1236
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-1905
dfn-cert: DFN-CERT-2016-1823
dfn-cert: DFN-CERT-2016-1407
dfn-cert: DFN-CERT-2016-1068
dfn-cert: DFN-CERT-2016-1059

High (CVSS: 7.5)

NVT: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.52
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow an attacker to conduct a denial-of-service condition.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.8 or 8.5.31 or 8.0.52 or 7.0.90 or later. Please see the references for more information.

Affected Software/OS
Apache Tomcat 9.0.0.M9 to 9.0.7 Apache Tomcat 8.5.0 to 8.5.30 Apache Tomcat 8.0.0.RC1 to 8.0.51 Apache Tomcat 7.0.28 to 7.0.86 on Windows.

Vulnerability Insight
The flaw exists due to improper handing of overflow in the UTF-8 decoder with supplementary characters.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat 'UTF-8 Decoder' Denial of Service Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.813724
Version used: 2025-09-17T05:39:26Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.107652)

References

```
cve: CVE-2018-1336
url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C201
↪80722090435.GA60759%40minotaur.apache.org%3E
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.8
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.31
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.52
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0809
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2018-2474
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2133
dfn-cert: DFN-CERT-2018-2125
dfn-cert: DFN-CERT-2018-2097
dfn-cert: DFN-CERT-2018-1928
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1541
dfn-cert: DFN-CERT-2018-1471
dfn-cert: DFN-CERT-2018-1443
dfn-cert: DFN-CERT-2018-1262
```

High (CVSS: 7.5)

NVT: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 8.0.33
Fixed version:     8.0.39
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: 8282/tcp

Impact
Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.

Solution:
Solution type: VendorFix
Upgrade to version 9.0.0.M17, 8.5.11 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M11 to 9.0.0.M15 and Apache Tomcat versions 8.5.0 to 8.5.9 on Windows.

Vulnerability Insight
The refactoring to make wider use of ByteBuffer introduced a regression that could cause information to leak between requests on the same connection. When running behind a reverse proxy, this could result in information leakage between users.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Reverse Proxy Information Disclosure Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.810719
Version used: 2024-02-15T05:05:40Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2016-8747
url: http://svn.apache.org/viewvc?view=revision&revision=1774161
url: http://www.securityfocus.com/bid/96895
url: http://svn.apache.org/viewvc?view=revision&revision=1774166
url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.11
url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M17
cert-bund: CB-K17/0426
dfn-cert: DFN-CERT-2017-0433

High (CVSS: 7.5)

NVT: Apache Tomcat Security Bypass Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.44
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow an attacker to exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:
Solution type: VendorFix
Upgrade to version 9.0.0.M21, or 8.5.15, or 8.0.44, or 7.0.78 or later.

Affected Software/OS
Apache Tomcat 9.0.0.M1 to 9.0.0.M20, Apache Tomcat 8.5.0 to 8.5.14, Apache Tomcat 8.0.0.RC1 to 8.0.43 and Apache Tomcat 7.0.0 to 7.0.77 on Windows

Vulnerability Insight
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. Tomcat's Default Servlet 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

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Security Bypass Vulnerability - Windows

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.811140
Version used: 2024-02-15T05:05:40Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2017-5664
url: https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b
↪8b7896538478d76066@%3Cannounce.tomcat.apache.org%3E
url: http://www.securityfocus.com/bid/98888
cert-bund: WID-SEC-2025-1212
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K18/0605
cert-bund: CB-K18/0603
cert-bund: CB-K18/0478
cert-bund: CB-K18/0066
cert-bund: CB-K18/0047
cert-bund: CB-K17/2024
cert-bund: CB-K17/2017
cert-bund: CB-K17/1831
cert-bund: CB-K17/1748
cert-bund: CB-K17/1492
cert-bund: CB-K17/1423
cert-bund: CB-K17/1257
cert-bund: CB-K17/1246
cert-bund: CB-K17/0977
dfn-cert: DFN-CERT-2018-1274
dfn-cert: DFN-CERT-2018-0729
dfn-cert: DFN-CERT-2018-0513
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2018-0051
dfn-cert: DFN-CERT-2017-2116
dfn-cert: DFN-CERT-2017-2106
dfn-cert: DFN-CERT-2017-1914
dfn-cert: DFN-CERT-2017-1827
dfn-cert: DFN-CERT-2017-1558
dfn-cert: DFN-CERT-2017-1485
dfn-cert: DFN-CERT-2017-1300
dfn-cert: DFN-CERT-2017-1288
dfn-cert: DFN-CERT-2017-1011

High (CVSS: 7.1)

NVT: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.39
Installation
path / port: 8282/tcp

Impact
Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.

Solution:
Solution type: VendorFix
Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.0.M11, Apache Tomcat versions 8.5.0 to 8.5.6, Apache Tomcat versions 8.0.0.RC1 to 8.0.38, Apache Tomcat versions 7.0.0 to 7.0.72, and Apache Tomcat versions 6.0.0 to 6.0.47 on Windows.

Vulnerability Insight
The code 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.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat HTTP Request Line Information Disclosure Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.810717
Version used: 2024-02-15T05:05:40Z

Product Detection Result
. . . continues on next page . . .

... continued from previous page ...

Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References

cve: CVE-2016-6816
url: https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48
url: http://www.securityfocus.com/bid/94461
url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13
url: https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-
↪information-disclosure
cert-bund: WID-SEC-2025-0215
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K17/1746
cert-bund: CB-K17/1060
cert-bund: CB-K17/1033
cert-bund: CB-K17/0444
cert-bund: CB-K17/0397
cert-bund: CB-K17/0198
cert-bund: CB-K17/0133
cert-bund: CB-K17/0090
cert-bund: CB-K16/1976
cert-bund: CB-K16/1927
cert-bund: CB-K16/1815
dfn-cert: DFN-CERT-2017-1822
dfn-cert: DFN-CERT-2017-1095
dfn-cert: DFN-CERT-2017-1068
dfn-cert: DFN-CERT-2017-0456
dfn-cert: DFN-CERT-2017-0404
dfn-cert: DFN-CERT-2017-0203
dfn-cert: DFN-CERT-2017-0137
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-2090
dfn-cert: DFN-CERT-2016-2035
dfn-cert: DFN-CERT-2016-1922

[return to 10.0.0.31]

2.1.2 High 80/tcp

High (CVSS: 10.0)

NVT: Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check

Product detection result
`cpe:/a:microsoft:internet_information_services:7.5`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: ↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Sends a special crafted HTTP GET request and checks the response.
Details: `Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2023-11-10T16:09:31Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`

. . . continues on next page . . .

... continued from previous page ...

Method: Microsoft Internet Information Services (IIS) Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
cve: CVE-2015-1635
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/topic/ms15-034-vulnerability-in-http-sy
↪s-could-allow-remote-code-execution-april-14-2015-e8755c1e-c5a8-fa75-c7b1-3208
↪7b127850
url: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2015/m
↪s15-034
url: http://pastebin.com/ypURDPc4
cert-bund: CB-K15/0527
dfn-cert: DFN-CERT-2015-0545

[return to 10.0.0.31]

2.1.3 High 1617/tcp

High (CVSS: 7.5)

NVT: Java JMX Insecure Configuration Vulnerability - Active Check

Summary
The Java JMX interface is configured in an insecure way by allowing unauthenticated attackers to load classes from any remote URL.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
It was possible to call 'javax.management.remote.rmi.RMIServer.newClient' on the
↪ RMI port 49239/tcp without providing any credentials.

Solution:
Solution type: Mitigation
Enable password authentication and/or SSL client certificate authentication for the JMX agent.

Vulnerability Detection Method
Sends crafted RMI requests and checks the responses.
Details: Java JMX Insecure Configuration Vulnerability - Active Check
OID:1.3.6.1.4.1.25623.1.0.143207
Version used: 2025-04-11T15:45:04Z

... continues on next page ...

... continued from previous page ...

References
url: https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/
url: https://www.optiv.com/blog/exploiting-jmx-rmi
url: https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server

[return to 10.0.0.31]

2.1.4 High 3000/tcp

High (CVSS: 9.8)

NVT: Ruby on Raily < 5.2.4.3, 6.x < 6.0.3.1 Multiple Vulnerabilities - Windows

Summary
Ruby on Rails is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 5.2.4.3
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 5.2.4.3 or 6.0.3.1 respectively.

Affected Software/OS
Ruby on Rails through version 5.2.4.2 and versions 6.0.0.0 through 6.0.3.0.

Vulnerability Insight
The following vulnerabilities exist:
- The Content-Length parameter of a direct file upload may be modified by an attacker to bypass upload limitations.
- A deserialization vulnerability may allow an attacker to read sensitive information.
- An attacker may unmarshal user-provided objects in MemCacheStore and RedisCacheStore resulting in arbitrary code execution.
- A cross-site request forgery (CSRF) vulnerability in the rails-ujs module may allow an attacker to perform actions in the context of another user.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: Ruby on Raily < 5.2.4.3, 6.x < 6.0.3.1 Multiple Vulnerabilities - Windows
OID:1.3.6.1.4.1.25623.1.0.113712
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2020-8162
cve: CVE-2020-8164
cve: CVE-2020-8165
cve: CVE-2020-8167
url: https://weblog.rubyonrails.org/2020/5/18/Rails-5-2-4-3-and-6-0-3-1-have-bee
↪n-released/
url: https://hackerone.com/reports/789579
url: https://hackerone.com/reports/292797
url: https://hackerone.com/reports/413388
url: https://hackerone.com/reports/189878
cert-bund: WID-SEC-2023-1093
cert-bund: CB-K20/0477
dfn-cert: DFN-CERT-2023-0981
dfn-cert: DFN-CERT-2021-0842
dfn-cert: DFN-CERT-2020-2327
dfn-cert: DFN-CERT-2020-2240
dfn-cert: DFN-CERT-2020-2093
dfn-cert: DFN-CERT-2020-2058
dfn-cert: DFN-CERT-2020-1582
dfn-cert: DFN-CERT-2020-1323

High (CVSS: 8.8)

NVT: Ruby on Rails < 5.0.1 RCE Vulnerability

Summary
Ruby on Rails is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 5.0.1
Installation
path / port: /

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target machine.

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Update to version 5.0.1 or later.

Affected Software/OS
Ruby on Rails through version 5.0.0.

Vulnerability Insight
An attacker may exploit this vulnerability by sending a specially crafted 'render' call.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails < 5.0.1 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113718
Version used: `2025-09-09T05:38:49Z`

References
`cve: CVE-2020-8163`
`url: https://hackerone.com/reports/304805`
`cert-bund: CB-K20/0472`
`dfn-cert: DFN-CERT-2020-1733`
`dfn-cert: DFN-CERT-2020-1582`

High (CVSS: 7.5)

NVT: Ruby on Rails Multiple Vulnerabilities (Jan 2016) - Windows

Summary
Ruby on Rails is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 4.1.1
Fixed version:     4.1.14.1
Installation
path / port:       /
```

Impact
Successful exploitation will allow a remote attacker to read arbitrary files by leveraging an application's unrestricted use of the render method, to cause a denial of service.

Solution:
Solution type: VendorFix
Update to version 3.2.22.1, 4.1.14.1, 4.2.5.1 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Ruby on Rails before 3.2.22.1, Ruby on Rails 4.0.x and 4.1.x before 4.1.14.1 and Ruby on Rails 4.2.x before 4.2.5.1 on Windows.

Vulnerability Insight
Multiple flaws are due to:
- Directory traversal vulnerability in Action View.
- The script 'actionpack/lib/action_dispatch/http/mime_type.rb' does not properly restrict use of the MIME type cache.
- The http_basic_authenticate_with method in 'actionpack/lib/action_controller/metal/http_authentication.rb' does not use a constant-time algorithm for verifying credentials.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Multiple Vulnerabilities (Jan 2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.809356
Version used: `2025-09-09T05:38:49Z`

References
`cve: CVE-2016-0752`
`cve: CVE-2016-0751`
`cve: CVE-2015-7576`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: http://www.openwall.com/lists/oss-security/2016/01/25/10`
`url: http://www.securityfocus.com/bid/81801`
`url: http://www.securityfocus.com/bid/81800`
`url: http://www.securityfocus.com/bid/81803`
`cert-bund: WID-SEC-2025-1085`
`cert-bund: CB-K17/0517`
`cert-bund: CB-K17/0278`
`cert-bund: CB-K16/0625`
`cert-bund: CB-K16/0522`
`cert-bund: CB-K16/0419`
`cert-bund: CB-K16/0238`
`cert-bund: CB-K16/0166`
`cert-bund: CB-K16/0165`
`dfn-cert: DFN-CERT-2017-0534`
`dfn-cert: DFN-CERT-2017-0284`
`dfn-cert: DFN-CERT-2016-0674`
`dfn-cert: DFN-CERT-2016-0566`
`dfn-cert: DFN-CERT-2016-0458`
`dfn-cert: DFN-CERT-2016-0259`
`dfn-cert: DFN-CERT-2016-0181`
`dfn-cert: DFN-CERT-2016-0178`

High (CVSS: 7.5)

NVT: Ruby on Rails Action Pack DoS Vulnerability (Jan 2016) - Windows

Summary
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 4.1.1
Fixed version:     4.2.5.1
Installation
path / port:       /
```

Impact
Successful exploitation will allow a remote attacker to cause a denial of service condition.

Solution:
Solution type: VendorFix
Update to version 4.2.5.1 or later.

Affected Software/OS
Ruby on Rails 4.x before 4.2.5.1 on Windows.

Vulnerability Insight
The flaw is due to an error in 'actionpack/lib/action_dispatch/routing/route_set.rb' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Action Pack DoS Vulnerability (Jan 2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.809362
Version used: `2025-09-09T05:38:49Z`

References
```
cve: CVE-2015-7581
url: http://www.openwall.com/lists/oss-security/2016/01/25/14
url: http://www.securityfocus.com/bid/81677
cert-bund: WID-SEC-2025-1085
cert-bund: CB-K16/0625
cert-bund: CB-K16/0419
cert-bund: CB-K16/0166
cert-bund: CB-K16/0165
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0181
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2016-0178

High (CVSS: 7.3)

NVT: Ruby on Rails Action Pack RCE Vulnerability (Feb 2016) - Windows

Summary
Ruby on Rails is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 4.1.14.2
Installation
path / port: /

Impact
Successful exploitation will allow a remote attacker to control the arguments of the render method in a controller or a view, resulting in the possibility of executing arbitrary ruby code.

Solution:
Solution type: VendorFix
Update to version 3.2.22.2, 4.1.14.2, 4.2.5.2 or later.

Affected Software/OS
Ruby on Rails before 3.2.22.2, Ruby on Rails 4.x before 4.1.14.2 and Ruby on Rails 4.2.x before 4.2.5.2 on Windows.

Vulnerability Insight
The flaw is due to an improper sanitization of user supplied inputs to the 'render' method in a controller or view by 'Action Pack'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Action Pack RCE Vulnerability (Feb 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809352
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2016-2098
url: https://www.debian.org/security/2016/dsa-3509
url: http://www.securityfocus.com/bid/83725
url: https://groups.google.com/g/rubyonrails-security/c/ly-IH-fxr_Q/m/WLoOhcMZIA
↪AJ

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-2271
cert-bund: CB-K17/1730
cert-bund: CB-K16/0625
cert-bund: CB-K16/0522
cert-bund: CB-K16/0426
cert-bund: CB-K16/0419
cert-bund: CB-K16/0372
dfn-cert: DFN-CERT-2017-1809
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0566
dfn-cert: DFN-CERT-2016-0468
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0404
```

[return to 10.0.0.31]

2.1.5 High 9200/tcp

High (CVSS: 10.0)

NVT: Elasticsearch End of Life (EOL) Detection

Summary
The Elasticsearch version on the remote host has reached the End of Life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The "Elasticsearch" version on the remote host has reached the end of life.
CPE:               cpe:/a:elastic:elasticsearch:1.1.1
Installed version: 1.1.1
EOL version:       1.1
EOL date:          2015-09-25
```

Impact
An EOL version of Elasticsearch is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: VendorFix
Update Elasticsearch to a version that still receives technical support and updates.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if an EOL version is present on the target host.
Details: `Elasticsearch End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.113131
Version used: `2025-09-03T08:26:15Z`

References
`url: https://www.elastic.co/support/eol`

High (CVSS: 9.8)

NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows

Summary
Elasticsearch is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 1.1.1`
`Fixed version: 1.6.1`

Impact
Successful exploitation will allow remote attackers to execute code or read arbitrary files.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.6.1, or later.

Affected Software/OS
Elasticsearch version 1.0.0 through 1.6.0 on Windows.

Vulnerability Insight
The Flaw is due to:
- an error in the snapshot API calls (CVE-2015-5531)
- an attack that can result in remote code execution (CVE-2015-5377).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.808091
Version used: `2025-09-03T08:26:15Z`

References
`cve: CVE-2015-5531`
`cve: CVE-2015-5377`

... continues on next page ...

... continued from previous page ...

```
url: https://www.elastic.co/community/security/
url: http://www.securityfocus.com/bid/75935
url: http://www.securityfocus.com/archive/1/archive/1/536017/100/0/threaded
cert-bund: WID-SEC-2025-2234
cert-bund: CB-K15/1118
dfn-cert: DFN-CERT-2025-2802
dfn-cert: DFN-CERT-2015-1160
```

High (CVSS: 8.8)

NVT: Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Windows

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 1.1.1`
`Fixed version: 5.6.12`

Impact
Successful exploitation would allow an authenticated attacker to acquire valid login credentials.

Solution:
Solution type: VendorFix
Update to version 5.6.12 or 6.4.1 respectively.

Affected Software/OS
Elasticsearch versions through 5.6.11 and 6.0.0 through 6.4.0.

Vulnerability Insight
The _cluster/settings API, when queried, could leak sensitive configuration information such as passwords, tokens or usernames.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Wi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.113276
Version used: `2025-09-03T08:26:15Z`

References
`cve: CVE-2018-3831`
`url: https://discuss.elastic.co/t/elastic-stack-6-4-1-and-5-6-12-security-update`

... continues on next page ...

... continued from previous page ...

```
↪/149035
url: https://www.elastic.co/community/security
dfn-cert: DFN-CERT-2025-2802
dfn-cert: DFN-CERT-2020-1653
```

[return to 10.0.0.31]

2.1.6 High 8022/tcp

High (CVSS: 10.0)

NVT: ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to obtain control over all connected active desktops via unspecified vectors.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 9.1.084
Fixed version:     10.0.082
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 10.0.082 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.082.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.082 Remote Control Privilege Violation Vuln.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106809
Version used: `2021-09-23T03:58:52Z`

References

```
cve: CVE-2017-7213
url: https://www.manageengine.com/products/desktop-central/cve-2017-7213-remote-
↪control-privilege-violation.html
```

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerability

Summary
ManageEngine Desktop Central 9 suffers from a vulnerability that allows a remote attacker to upload a malicious file, and execute it under the context of SYSTEM.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
`It was possible to upload the file ‘http://10.0.0.31:8022/jspf/OpenVASVT_CVE-201 ↪5-8249_test.jsp‘. Please delete this file.`

Impact
Successful exploitation will allow an attacker to gain arbitrary code execution on the server.

Solution:
Solution type: VendorFix
Update to version 9.0.142 or later.

Affected Software/OS
ManageEngine Desktop Central prior to version 9.0.142.

Vulnerability Detection Method
Try to upload a jsp file.
Details: `ManageEngine Desktop Central < 9.0.142 FileUploadServlet connectionId Vulnerabi. ↪..`
OID:1.3.6.1.4.1.25623.1.0.140041
Version used: `2021-10-12T12:01:25Z`

References
`cve: CVE-2015-8249`

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure Vulnerability

Summary
ManageEngine Desktop Central is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 9.1.084
Fixed version:     10.0.157
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to download unencrypted XML files containing all data for configuration policies.

Solution:
Solution type: VendorFix
Update to version 10.0.157 or later.

Affected Software/OS
ManageEngine Desktop Central/MSP version 10.0.137 and prior.

Vulnerability Insight
This issue exists in an unknown function of the file '/client-data//collections/##/usermgmt.xml'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 10.0.137 'usermgmt.xml' Information Disclosure ...`
OID:1.3.6.1.4.1.25623.1.0.812522
Version used: `2023-01-19T10:10:48Z`

References
`cve: CVE-2017-16924`
`url: https://www.manageengine.com/desktop-management-msp/password-encryption-policy-violation.html`

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple vulnerabilities.

Quality of Detection (QoD): 100%

Vulnerability Detection Result
`Vulnerable URL: http://10.0.0.31:8022/jsp/admin/DBQueryExecutor.jsp?actionFrom=getResult&query=SELECT%20*%20from%20aaauser;`

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation will allow attackers to write arbitrary files, gain access to unrestricted resources and execute remote code.

Solution:
Solution type: VendorFix
Update to version 10.0.208 or later.

Affected Software/OS
ManageEngine Desktop Central version 10.0.184 and prior.

Vulnerability Insight
Multiple flaws are due to:
- The missing authentication/authorization on a database query mechanism.
- An insufficient enforcement of database query type restrictions.
- The missing server side check on file type/extension when uploading and modifying scripts
- The directory traversal in SCRIPT_NAME field when modifying existing scripts

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `ManageEngine Desktop Central <= 10.0.184 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.813213
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2018-5337`
`cve: CVE-2018-5338`
`cve: CVE-2018-5339`
`cve: CVE-2018-5341`
`url: https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vuln`
`↪erabilities-in-manageengine-desktop-central`

High (CVSS: 9.8)

NVT: ManageEngine Desktop Central < 10.0.092 RCE Vulnerability

Summary
ManageEngine Desktop Central allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 9.1.084`
`Fixed version: 10.0.092`

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        /
```

Solution:
Solution type: VendorFix
Update to version 10.0.092 or later.

Affected Software/OS
ManageEngine Desktop Central before version 10.0.092.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central < 10.0.092 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.106969
Version used: `2021-09-23T03:58:52Z`

References
`cve: CVE-2017-11346`
`url: https://www.manageengine.com/products/desktop-central/remote-code-execution.html`

[return to 10.0.0.31]

2.1.7 High 445/tcp

High (CVSS: 8.8)

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2024-07-17T05:05:38Z`

References
`cve: CVE-2017-0143`
`cve: CVE-2017-0144`
`cve: CVE-2017-0145`
`cve: CVE-2017-0146`
`cve: CVE-2017-0147`
`cve: CVE-2017-0148`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`url: https://support.microsoft.com/en-us/kb/4013078`
`url: http://www.securityfocus.com/bid/96703`
`url: http://www.securityfocus.com/bid/96704`
`url: http://www.securityfocus.com/bid/96705`
`url: http://www.securityfocus.com/bid/96707`
`url: http://www.securityfocus.com/bid/96709`
`url: http://www.securityfocus.com/bid/96706`
`url: https://technet.microsoft.com/library/security/MS17-010`
`url: https://github.com/rapid7/metasploit-framework/pull/8167/files`
`cert-bund: CB-K17/0435`
`dfn-cert: DFN-CERT-2017-0448`

[return to 10.0.0.31]

2.1.8 High 21/tcp

High (CVSS: 7.5) NVT: FTP Brute Force Logins With Default Credentials Reporting
Summary It was possible to login into the remote FTP server using weak/known credentials.
Quality of Detection (QoD): 95%

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`vagrant:vagrant`

Impact This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.
Solution: **Solution type:** Mitigation Change the password as soon as possible.
Vulnerability Insight The following devices are / software is known to be affected: - CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R - CVE-2013-7404: GE Healthcare Discovery NM 750b - CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways - CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station - CVE-2016-8731: Foscam C1 devices - CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices - CVE-2018-9068: IMM2 for IBM and Lenovo System x - CVE-2018-17771: Ingenico Telium 2 PoS terminals - CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices Note: As the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
Vulnerability Detection Method Reports weak/known credentials detected by the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717). Details: `FTP Brute Force Logins With Default Credentials Reporting` OID:1.3.6.1.4.1.25623.1.0.108718 Version used: `2025-05-13T05:41:39Z`
References

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2014-9198
cve: CVE-2015-7261
cve: CVE-2016-8731
cve: CVE-2017-8218
cve: CVE-2018-9068
cve: CVE-2018-17771
cve: CVE-2018-19063
cve: CVE-2018-19064
```

[return to 10.0.0.31]

2.1.9 High 22/tcp

High (CVSS: 9.8)

NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`vagrant:vagrant`

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Affected Software/OS
The following products are known to use the default credentials checked by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) used for this reporting:

... continues on next page ...

... continued from previous page ...

- CVE-2017-16523: MitraStar GPT-2541GNAC (HGU) 1.00(VNJ0)b1 and DSL-100HN-T1 ES_113WJY0b16 devices
- CVE-2020-29583: Zyxel Firewall / AP Controller
- CVE-2020-9473: S. Siedle & Soehne SG 150-0 Smart Gateway before 1.2.4
- CVE-2021-27797: Brocade Fabric OS
- CVE-2023-1944: minikube 1.29.0 and probably prior
- CVE-2024-22902: Vinchin Backup & Recovery
- CVE-2024-31970: AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1) during a window of time when the device is being set up
- CVE-2024-46328: VONETS VAP11G-300 v3.3.23.6.9
- Various additional products like e.g. Ubiquiti EdgeMax / EdgeRouter, Crestron AM-100 and similar for which no CVE was assigned (See 'default_credentials.inc' file on the file system for a full list)

Other products might be affected as well.

Vulnerability Insight

As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).

Details: `SSH Brute Force Logins With Default Credentials Reporting`

OID:1.3.6.1.4.1.25623.1.0.103239

Version used: `2025-04-04T05:39:39Z`

References

`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2005-1379`
`cve: CVE-2006-5288`
`cve: CVE-2009-3710`
`cve: CVE-2012-4577`
`cve: CVE-2016-1000245`
`cve: CVE-2017-16523`
`cve: CVE-2020-29583`
`cve: CVE-2020-9473`
`cve: CVE-2021-27797`
`cve: CVE-2023-1944`
`cve: CVE-2024-22902`
`cve: CVE-2024-31970`
`cve: CVE-2024-46328`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`cisa: Known Exploited Vulnerability (KEV) catalog`

High (CVSS: 9.8)

NVT: OpenSSH < 7.2 X11 Forwarding Security Bypass Vulnerability - Windows

Product detection result
`cpe:/a:openbsd:openssh:7.1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

Summary
OpenSSH is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: 7.2`
`Installation path / port: 22/tcp`

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:
Solution type: VendorFix
Update to version 7.2 or later.

Affected Software/OS
OpenSSH versions before 7.2 on Windows.

Vulnerability Insight
An access flaw was discovered in OpenSSH, it did not correctly handle failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X application could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forwarding was requested.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.2 X11 Forwarding Security Bypass Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.810768
Version used: `2024-12-13T05:05:32Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2016-1908
url: http://openwall.com/lists/oss-security/2016/01/15/13
url: http://www.securityfocus.com/bid/84427
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
url: http://www.openssh.com/txt/release-7.2
url: https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0
↪db113c71e234416c
url: https://bugzilla.redhat.com/show_bug.cgi?id=1298741
cert-bund: CB-K16/1485
cert-bund: CB-K16/0694
cert-bund: CB-K16/0684
cert-bund: CB-K16/0449
cert-bund: CB-K16/0162
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-0754
dfn-cert: DFN-CERT-2016-0733
dfn-cert: DFN-CERT-2016-0488
dfn-cert: DFN-CERT-2016-0182
```

High (CVSS: 7.8)

NVT: OpenSSH < 7.4 Multiple Vulnerabilities (Jan 2017) - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     7.4
Installation
path / port:       22/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution:
Solution type: VendorFix
Update to version 7.4 or later.

Affected Software/OS
OpenSSH versions before 7.4 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- An 'authfile.c' script does not properly consider the effects of realloc on buffer contents.
- The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers.
- The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used.
- An untrusted search path vulnerability in ssh-agent.c in ssh-agent.
- NULL pointer dereference error due to an out-of-sequence NEWKEYS message.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.4 Multiple Vulnerabilities (Jan 2017) - Windows`
OID:1.3.6.1.4.1.25623.1.0.810325
Version used: `2024-12-13T05:05:32Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2016-10009`
`cve: CVE-2016-10010`
`cve: CVE-2016-10011`
`cve: CVE-2016-10012`
`cve: CVE-2016-10708`
`url: https://www.openssh.com/txt/release-7.4`
`url: http://www.securityfocus.com/bid/94968`
`url: http://www.securityfocus.com/bid/94972`
`url: http://www.securityfocus.com/bid/94977`
`url: http://www.securityfocus.com/bid/94975`
`url: http://www.openwall.com/lists/oss-security/2016/12/19/2`
`url: http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html`

... continues on next page ...

... continued from previous page ...

```
url: https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e93
↪3e6b931de1d16737
cert-bund: WID-SEC-2023-1996
cert-bund: CB-K18/0919
cert-bund: CB-K18/0591
cert-bund: CB-K18/0137
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1292
cert-bund: CB-K17/1061
cert-bund: CB-K17/0527
cert-bund: CB-K17/0377
cert-bund: CB-K17/0127
cert-bund: CB-K17/0041
cert-bund: CB-K16/1991
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-2068
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1568
dfn-cert: DFN-CERT-2018-1432
dfn-cert: DFN-CERT-2018-1112
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-1068
dfn-cert: DFN-CERT-2018-0150
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-1096
dfn-cert: DFN-CERT-2017-0532
dfn-cert: DFN-CERT-2017-0386
dfn-cert: DFN-CERT-2017-0130
dfn-cert: DFN-CERT-2017-0042
dfn-cert: DFN-CERT-2016-2099
```

High (CVSS: 7.5)

NVT: OpenSSH < 7.3 DoS and User Enumeration Vulnerabilities - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

... continues on next page ...

... continued from previous page ...

Summary
OpenSSH is prone to denial of service (DoS) and user enumeration vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: 7.3`
`Installation path / port: 22/tcp`

Impact
Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution:
Solution type: VendorFix
Update to version 7.3 or later.

Affected Software/OS
OpenSSH versions before 7.3 on Windows.

Vulnerability Insight
Multiple flaws exist due to:
- The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication.
- The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.3 DoS and User Enumeration Vulnerabilities - Windows`
OID:1.3.6.1.4.1.25623.1.0.809121
Version used: `2024-12-13T05:05:32Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2016-6515
cve: CVE-2016-6210
url: http://www.openssh.com/txt/release-7.3
url: http://www.securityfocus.com/bid/92212
url: http://seclists.org/fulldisclosure/2016/Jul/51
url: https://security-tracker.debian.org/tracker/CVE-2016-6210
url: http://openwall.com/lists/oss-security/2016/08/01/2
cert-bund: WID-SEC-2023-0450
cert-bund: WID-SEC-2023-0449
cert-bund: CB-K18/0041
cert-bund: CB-K17/2219
cert-bund: CB-K17/2112
cert-bund: CB-K17/1753
cert-bund: CB-K17/1349
cert-bund: CB-K17/1292
cert-bund: CB-K17/0055
cert-bund: CB-K16/1837
cert-bund: CB-K16/1629
cert-bund: CB-K16/1487
cert-bund: CB-K16/1485
cert-bund: CB-K16/1252
cert-bund: CB-K16/1221
cert-bund: CB-K16/1082
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2018-1828
dfn-cert: DFN-CERT-2018-1070
dfn-cert: DFN-CERT-2018-0046
dfn-cert: DFN-CERT-2017-2320
dfn-cert: DFN-CERT-2017-2208
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1407
dfn-cert: DFN-CERT-2017-1340
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1729
dfn-cert: DFN-CERT-2016-1576
dfn-cert: DFN-CERT-2016-1574
dfn-cert: DFN-CERT-2016-1331
dfn-cert: DFN-CERT-2016-1243
dfn-cert: DFN-CERT-2016-1149
```

[return to 10.0.0.31]

2.1.10 Medium 8282/tcp

Medium (CVSS: 6.8)

NVT: Apache Tomcat servlet/JSP container default files

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
The Apache Tomcat servlet/JSP container has default files installed.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The following default files were found :
http://10.0.0.31:8282/examples/servlets/index.html
http://10.0.0.31:8282/examples/jsp/snp/snoop.jsp
http://10.0.0.31:8282/examples/jsp/index.html

Impact
These files should be removed as they may help an attacker to guess the exact version of the Apache Tomcat which is running on this host and may provide other useful information.

Solution:
Solution type: Mitigation
Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

Vulnerability Insight
Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.

Vulnerability Detection Method
Details: Apache Tomcat servlet/JSP container default files
OID:1.3.6.1.4.1.25623.1.0.12085
Version used: 2023-08-01T13:29:10Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

Medium (CVSS: 6.5)

NVT: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilities - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to multiple access bypass vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.0.50
Installation
path / port: 8282/tcp

Impact
Successfully exploiting these issues will allow remote attackers to bypass security constraints to access ostensibly restricted resources on the target system.

Solution:
Solution type: VendorFix
Upgrade to Apache Tomcat version 9.0.5, 8.5.28, 8.0.50, 7.0.85 or later.

Affected Software/OS
Apache Tomcat versions 9.0.0.M1 to 9.0.4
Apache Tomcat versions 8.5.0 to 8.5.27
Apache Tomcat versions 8.0.0.RC1 to 8.0.49
Apache Tomcat versions 7.0.0 to 7.0.84 on Windows.

Vulnerability Insight
Multiple flaws are due to:
- The system does not properly enforce security constraints that defined by annotations of Servlets in certain cases, depending on the order that Servlets are loaded.
- The URL pattern of " (the empty string) which exactly maps to the context root was not correctly handled when used as part of a security constraint definition.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Security Constraint Incorrect Handling Access Bypass Vulnerabilit.

. . . continues on next page . . .

... continued from previous page ...

↪..
OID:1.3.6.1.4.1.25623.1.0.812784
Version used: 2025-09-17T05:39:26Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2018-1305
cve: CVE-2018-1304
url: http://tomcat.apache.org/security-9.html
url: http://www.securityfocus.com/bid/103144
url: http://www.securityfocus.com/bid/103170
url: http://tomcat.apache.org/security-8.html
url: http://tomcat.apache.org/security-7.html
url: https://lists.apache.org/thread.html/b1d7e2425d6fd2cebed40d318f9365b4454607
↪7e10949b01b1f8a0fb@%3Cannounce.tomcat.apache.org%3E
cert-bund: WID-SEC-2024-1682
cert-bund: WID-SEC-2024-0528
cert-bund: CB-K19/1121
cert-bund: CB-K19/0321
cert-bund: CB-K18/1007
cert-bund: CB-K18/1006
cert-bund: CB-K18/1005
cert-bund: CB-K18/0790
cert-bund: CB-K18/0420
cert-bund: CB-K18/0349
dfn-cert: DFN-CERT-2019-1627
dfn-cert: DFN-CERT-2019-0772
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2125
dfn-cert: DFN-CERT-2018-2103
dfn-cert: DFN-CERT-2018-1753
dfn-cert: DFN-CERT-2018-1407
dfn-cert: DFN-CERT-2018-1274
dfn-cert: DFN-CERT-2018-1253
dfn-cert: DFN-CERT-2018-1038
dfn-cert: DFN-CERT-2018-0922
dfn-cert: DFN-CERT-2018-0733
dfn-cert: DFN-CERT-2018-0455
dfn-cert: DFN-CERT-2018-0378

Medium (CVSS: 6.4)

NVT: Apache Axis2 <= 1.6.2 Multiple Vulnerabilities

Summary
Apache Axis2 is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.6.0
Fixed version:     None
Installation
path / port:       /axis2
```

Impact
Successfully exploiting these issues allows attackers to:
- CVE-2012-5785: perform man-in-the-middle attacks or impersonate trusted servers, which will aid in further attacks
- CVE-2012-4418: may allow unauthenticated attackers to construct specially crafted messages that can be successfully verified and contain arbitrary content. This may aid in further attacks
- CVE-2012-5351: allows remote attackers to forge messages and bypass authentication

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
The issue affects versions up to 1.6.2.

Vulnerability Insight
The following flaws exist:
- CVE-2012-5785: a security bypass vulnerability because the application fails to properly validate SSL certificates from the server
- CVE-2012-4418: a security vulnerability involving XML signature wrapping
- CVE-2012-5351: a SAML assertion that lacks a Signature element, aka a 'Signature exclusion attack'

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Axis2 <= 1.6.2 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.111004
Version used: `2025-01-17T15:39:18Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References
cve: CVE-2012-5785
cve: CVE-2012-4418
cve: CVE-2012-5351
url: https://issues.apache.org/jira/browse/AXIS2C-1607
url: http://www.securityfocus.com/bid/56408
url: http://www.securityfocus.com/bid/55508

Medium (CVSS: 6.4)

NVT: Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to an authentication bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 9.0.96
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 9.0.96, 10.1.31, 11.0.0 or later.

Affected Software/OS
Apache Tomcat versions prior to 9.0.96, 10.0.x through 10.1.30 and 11.0.0-M1 through 11.0.0-M26.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

If Tomcat was configured to use a custom Jakarta Authentication (formerly JASPIC) ServerAuthContext component which may throw an exception during the authentication process without explicitly setting an HTTP status to indicate failure, the authentication may not have failed, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows`
OID:1.3.6.1.4.1.25623.1.0.153463
Version used: `2024-12-19T05:05:34Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2024-52316`
`url: https://lists.apache.org/thread/lopzlqh91jj9n334g02om08sbysdb928`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.31`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.96`
`cert-bund: WID-SEC-2025-0521`
`cert-bund: WID-SEC-2024-3684`
`cert-bund: WID-SEC-2024-3486`
`dfn-cert: DFN-CERT-2025-2285`
`dfn-cert: DFN-CERT-2025-2098`
`dfn-cert: DFN-CERT-2025-0890`
`dfn-cert: DFN-CERT-2025-0146`
`dfn-cert: DFN-CERT-2025-0134`
`dfn-cert: DFN-CERT-2024-3156`
`dfn-cert: DFN-CERT-2024-3077`

Medium (CVSS: 5.0)

NVT: Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows

Product detection result
`cpe:/a:apache:tomcat:8.0.33`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`
`↪7652)`

Summary

... continues on next page ...

... continued from previous page ...

Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 8.5.99`
`Installation path / port: 8282/tcp`

Solution:
Solution type: VendorFix
Update to version 8.5.99, 9.0.86, 10.1.19, 11.0.0-M17 or later.

Affected Software/OS
Apache Tomcat versions prior to 8.5.99, 9.0.0-M1 through 9.0.85, 10.x through 10.1.18 and 11.0.0-M1 through 11.0.0-M16.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 8.5.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
The following flaws exist:
- CVE-2024-23672: WebSocket DoS with incomplete closing handshake
- CVE-2024-24549: HTTP/2 header handling DoS

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows`
OID:1.3.6.1.4.1.25623.1.0.114428
Version used: `2024-12-19T05:05:34Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2024-23672`
`cve: CVE-2024-24549`
`url: https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f`
`url: https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M1`
`↪7`

... continues on next page ...

... continued from previous page ...

```
url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.19
url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.86
url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.99
url: https://nowotarski.info/http2-continuation-flood/
url: https://nowotarski.info/http2-continuation-flood-technical-details/
cert-bund: WID-SEC-2024-3663
cert-bund: WID-SEC-2024-3508
cert-bund: WID-SEC-2024-3377
cert-bund: WID-SEC-2024-3220
cert-bund: WID-SEC-2024-3219
cert-bund: WID-SEC-2024-3196
cert-bund: WID-SEC-2024-3195
cert-bund: WID-SEC-2024-3191
cert-bund: WID-SEC-2024-1656
cert-bund: WID-SEC-2024-1642
cert-bund: WID-SEC-2024-1638
cert-bund: WID-SEC-2024-1622
cert-bund: WID-SEC-2024-1238
cert-bund: WID-SEC-2024-1214
cert-bund: WID-SEC-2024-1210
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0630
dfn-cert: DFN-CERT-2025-1517
dfn-cert: DFN-CERT-2024-3096
dfn-cert: DFN-CERT-2024-3078
dfn-cert: DFN-CERT-2024-2743
dfn-cert: DFN-CERT-2024-1846
dfn-cert: DFN-CERT-2024-1372
dfn-cert: DFN-CERT-2024-1235
dfn-cert: DFN-CERT-2024-1036
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0723
dfn-cert: DFN-CERT-2024-0722
dfn-cert: DFN-CERT-2024-0697
```

Medium (CVSS: 5.0)

NVT: Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows

Product detection result

```
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)
```

Summary

... continues on next page ...

... continued from previous page ...

Apache Tomcat is prone to a CGI security constraint bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 8.0.33`
`Fixed version: 9.0.105`
`Installation path / port: 8282/tcp`

Solution:
Solution type: VendorFix
Update to version 9.0.105, 10.1.41, 11.0.7 or later.

Affected Software/OS
Apache Tomcat version 9.0.104 and prior, 10.x through 10.1.40 and 11.0.0-M1 through 11.0.6.
Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
When running on a case insensitive file system with security constraints configured for the <code>pathInfo</code> component of a URL that mapped to the CGI servlet, it is possible to bypass those security constraints with a specially crafted URL.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows`
OID:1.3.6.1.4.1.25623.1.0.154591
Version used: `2025-05-30T15:42:19Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2025-46701`
`url: https://lists.apache.org/thread/xhqqk9w5q45srcdqhogdk04lhdscv30j`
`cert-bund: WID-SEC-2025-1850`
`cert-bund: WID-SEC-2025-1365`
`cert-bund: WID-SEC-2025-1165`
`dfn-cert: DFN-CERT-2025-2285`
`dfn-cert: DFN-CERT-2025-2098`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2025-1991
dfn-cert: DFN-CERT-2025-1905
dfn-cert: DFN-CERT-2025-1780
dfn-cert: DFN-CERT-2025-1384

Medium (CVSS: 5.0)

NVT: Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
Apache Tomcat is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 9.0.98
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 9.0.98, 10.1.34, 11.0.2 or later.
Vendor note: Users running Tomcat on a case insensitive file system with the default servlet write enabled (readonly initialisation parameter set to the non-default value of false) may need additional configuration to fully mitigate CVE-2024-50379 depending on which version of Java they are using with Tomcat:
- running on Java 8 or Java 11: the system property sun.io.useCanonCaches must be explicitly set to false (it defaults to true)
- running on Java 17: the system property sun.io.useCanonCaches, if set, must be set to false (it defaults to false)
- running on Java 21 onwards: no further configuration is required (the system property and the problematic cache have been removed)

Affected Software/OS
Apache Tomcat versions prior to 9.0.98, 10.x prior to 10.1.34 and 11.x prior to 11.0.2.

... continues on next page ...

... continued from previous page ...

Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Vulnerability Insight
The following flaws exist:
- CVE-2024-50379: Remote code execution (RCE) via write-enabled default servlet
- CVE-2024-54677: Denial of service (DoS) in examples web application
- CVE-2024-56337: RCE via write-enabled default servlet - CVE-2024-50379 mitigation was incomplete

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows`
OID:1.3.6.1.4.1.25623.1.0.114890
Version used: `2024-12-24T05:05:31Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2024-50379`
`cve: CVE-2024-54677`
`cve: CVE-2024-56337`
`url: https://lists.apache.org/thread/y6lj6q1xnp822g6ro70tn19sgtjmr80r`
`url: https://lists.apache.org/thread/tdtbbxpg5trdwc2wnopcth9ccvdftq2n`
`url: https://lists.apache.org/thread/b2b9qrgjrz1kvo4ym8y2wkfdvwoq6qbp`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98`
`cert-bund: WID-SEC-2025-0823`
`cert-bund: WID-SEC-2025-0819`
`cert-bund: WID-SEC-2025-0818`
`cert-bund: WID-SEC-2025-0808`
`cert-bund: WID-SEC-2025-0719`
`cert-bund: WID-SEC-2025-0148`
`cert-bund: WID-SEC-2024-3744`
`cert-bund: WID-SEC-2024-3722`
`dfn-cert: DFN-CERT-2025-2285`
`dfn-cert: DFN-CERT-2025-2098`
`dfn-cert: DFN-CERT-2025-1991`
`dfn-cert: DFN-CERT-2025-1923`
`dfn-cert: DFN-CERT-2025-1181`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2025-0974
dfn-cert: DFN-CERT-2025-0890
dfn-cert: DFN-CERT-2025-0888
dfn-cert: DFN-CERT-2025-0766
dfn-cert: DFN-CERT-2025-0528
dfn-cert: DFN-CERT-2025-0509
dfn-cert: DFN-CERT-2025-0444
dfn-cert: DFN-CERT-2025-0146
dfn-cert: DFN-CERT-2025-0138
dfn-cert: DFN-CERT-2025-0134
dfn-cert: DFN-CERT-2025-0036
dfn-cert: DFN-CERT-2024-3364
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://10.0.0.31:8282/host-manager/html:"Tomcat Host Manager Application"
http://10.0.0.31:8282/manager/html:"Tomcat Manager Application"
http://10.0.0.31:8282/manager/status:"Tomcat Manager Application"
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

Medium (CVSS: 4.3)

NVT: Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows

Product detection result
`cpe:/a:apache:tomcat:8.0.33`
`Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10`
`↪7652)`

Summary
Apache Tomcat is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 8.0.33
Fixed version:     8.5.86
Installation
path / port:       8282/tcp
```

Solution:
Solution type: VendorFix
Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.

Affected Software/OS
Apache Tomcat versions through 8.5.85, 9.0.0-M1 through 9.0.71, 10.x through 10.1.5 and 11.0.0-M1 through 11.0.0-M2.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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 Tomcat did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows`
OID:1.3.6.1.4.1.25623.1.0.104654
Version used: `2024-06-07T05:05:42Z`

Product Detection Result
Product: `cpe:/a:apache:tomcat:8.0.33`
Method: `Apache Tomcat Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
`cve: CVE-2023-28708`
`url: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67`
`url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3`
`url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.6`
`url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.72`
`url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86`
`cert-bund: WID-SEC-2024-1238`
`cert-bund: WID-SEC-2024-0528`
`cert-bund: WID-SEC-2023-2674`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1808`
`cert-bund: WID-SEC-2023-1784`
`cert-bund: WID-SEC-2023-1783`
`cert-bund: WID-SEC-2023-1782`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1021`
`cert-bund: WID-SEC-2023-1017`
`cert-bund: WID-SEC-2023-0717`
`dfn-cert: DFN-CERT-2025-1517`
`dfn-cert: DFN-CERT-2024-3078`
`dfn-cert: DFN-CERT-2023-2778`
`dfn-cert: DFN-CERT-2023-2545`
`dfn-cert: DFN-CERT-2023-2054`
`dfn-cert: DFN-CERT-2023-0772`
`dfn-cert: DFN-CERT-2023-0763`
`dfn-cert: DFN-CERT-2023-0640`

Medium (CVSS: 4.3)

NVT: Apache Tomcat Open Redirect Vulnerability - Windows

Product detection result
cpe:/a:apache:tomcat:8.0.33
Detected by Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.10
↪7652)

Summary
When the default servlet in Apache Tomcat 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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 8.0.33
Fixed version: 8.5.34
Installation
path / port: 8282/tcp

Solution:
Solution type: VendorFix
Update to version 7.0.91, 8.5.34, 9.0.12 or later.

Affected Software/OS
Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache Tomcat Open Redirect Vulnerability - Windows
OID:1.3.6.1.4.1.25623.1.0.141569
Version used: 2024-02-15T05:05:40Z

Product Detection Result
Product: cpe:/a:apache:tomcat:8.0.33
Method: Apache Tomcat Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.107652)

References
cve: CVE-2018-11784
url: http://tomcat.apache.org/security-9.html
url: http://tomcat.apache.org/security-8.html

... continues on next page ...

... continued from previous page ...

```
url: http://tomcat.apache.org/security-7.html
cert-bund: WID-SEC-2025-1212
cert-bund: WID-SEC-2024-1682
cert-bund: WID-SEC-2024-0528
cert-bund: WID-SEC-2023-0531
cert-bund: WID-SEC-2023-0460
cert-bund: CB-K20/0029
cert-bund: CB-K19/1121
cert-bund: CB-K19/0907
cert-bund: CB-K19/0616
cert-bund: CB-K19/0320
cert-bund: CB-K19/0050
cert-bund: CB-K18/0963
dfn-cert: DFN-CERT-2019-2710
dfn-cert: DFN-CERT-2019-2159
dfn-cert: DFN-CERT-2019-1562
dfn-cert: DFN-CERT-2019-1237
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0147
dfn-cert: DFN-CERT-2019-0104
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2165
dfn-cert: DFN-CERT-2018-2142
dfn-cert: DFN-CERT-2018-2000
```

[return to 10.0.0.31]

2.1.11 Medium 4848/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Quality of Detection (QoD): 99%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=GlassFish,O=Oracle Corporation,L=Santa Clara,ST=Californ
↪ia,C=US
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Impact

An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `2024-06-14T05:05:48Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security`

Method: `SSL/TLS: Collect and Report Certificate Details`

OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service expired on 2023-05-13 05:33:38.
Certificate details:
fingerprint (SHA-1)             | 4A5758F59279E82F2A913C83CA658D6964575A72
fingerprint (SHA-256)           | AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD
↪5B23381002A885F556
issued by                       | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 04A9972F
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=GlassFish,O=Oracle Corporation
↪,L=Santa Clara,ST=California,C=US
subject alternative names (SAN) | None
valid from                      | 2013-05-15 05:33:38 UTC
valid until                     | 2023-05-13 05:33:38 UTC
```

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: 2024-06-14T05:05:48Z

. . . continues on next page . . .

... continued from previous page ...

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols.
Please see the references for more resources supporting you with this task.

Affected Software/OS
- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols
- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder
- CVE-2024-41270: Gorush v1.18.4
- CVE-2025-3200: Multiple products from Wiesemann & Theis

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Checks the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2025-04-30T05:39:51Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

References
`cve: CVE-2011-3389`
`cve: CVE-2015-0204`
`cve: CVE-2023-41928`
`cve: CVE-2024-41270`
`cve: CVE-2025-3200`
`url: https://ssl-config.mozilla.org`
`url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel`
`↪ines/TG02102/BSI-TR-02102-1.html`
`url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/`
`↪TLS-Protokoll/TLS-Protokoll_node.html`
`url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch`
`↪eRichtlinien/TR03116/BSI-TR-03116-4.html`
`url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes`
`↪tstandard_BSI_TLS_Version_2_4.html`
`url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org`
`url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters`
`↪-report-2014`
`url: https://datatracker.ietf.org/doc/rfc8996/`
`url: https://vnhacker.blogspot.com/2011/09/beast.html`
`url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
`url: https://certvde.com/en/advisories/VDE-2025-031/`
`url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc`
`url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K18/0799`
`cert-bund: CB-K16/1289`
`cert-bund: CB-K16/1096`
`cert-bund: CB-K15/1751`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619

... continues on next page ...

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2011-1482

[return to 10.0.0.31]

2.1.12 Medium 3000/tcp

Medium (CVSS: 6.5)

NVT: Ruby on Rails < 6.0.3.2 DoS Vulnerability

Summary
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 6.0.3.2
Installation
path / port: /

Impact
Successful exploitation would allow an attacker to render legitimate users unable to use the application.

Solution:
Solution type: VendorFix
Update to version 6.0.3.2 or later.

Affected Software/OS
Ruby on Rails through version 6.0.3.1.

Vulnerability Insight
An untrusted user may run any pending migration in production.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails < 6.0.3.2 DoS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.113716
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2020-8185
url: https://hackerone.com/reports/899069

. . . continues on next page . . .

... continued from previous page ...

cert-bund: CB-K20/0604
dfn-cert: DFN-CERT-2021-0842
dfn-cert: DFN-CERT-2020-2327

Medium (CVSS: 6.1)

NVT: Ruby on Rails Action View XSS Vulnerability (Aug 2016) - Windows

Summary
Ruby on Rails is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 4.2.7.1
Installation
path / port: /

Impact
Successful exploitation will allow a remote attacker to inject arbitrary web script or HTML via crafted parameters.

Solution:
Solution type: VendorFix
Update to version 3.2.22.3, 4.2.7.1, 5.0.0.1 or later.

Affected Software/OS
Ruby on Rails 3.x before 3.2.22.3, Ruby on Rails 4.x before 4.2.7.1 and Ruby on Rails 5.x before 5.0.0.1 on Windows.

Vulnerability Insight
The flaw is due to the Text declared as 'HTML safe' when passed as an attribute value to a tag helper will not have quotes escaped which can lead to an XSS attack.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Action View XSS Vulnerability (Aug 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.807379
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2016-6316
url: http://seclists.org/oss-sec/2016/q3/260
url: http://www.securityfocus.com/bid/92430

... continues on next page ...

... continued from previous page ...

```
url: https://groups.google.com/forum/#!msg/rubyonrails-security/I-VWr034ouk/gGu2
↪FrCwDAAJ
url: http://weblog.rubyonrails.org/2016/8/11/Rails-5-0-0-1-4-2-7-2-and-3-2-22-3-
↪have-been-released
cert-bund: CB-K17/1730
cert-bund: CB-K16/1256
dfn-cert: DFN-CERT-2017-1809
dfn-cert: DFN-CERT-2016-1321
```

Medium (CVSS: 5.9)

NVT: Ruby on Rails Information Disclosure Vulnerability (GHSA-rmj8-8hhh-gv5h) - Windows

Summary
Ruby on Rails is prone to an information disclosure vulnerability in puma.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 4.1.1
Fixed version:     5.2.6.2
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 5.2.6.2, 6.0.4.6, 6.1.4.6, 7.0.2.2 or later.

Affected Software/OS
Ruby on Rails version 5.x through 7.0.x.

Vulnerability Insight
Puma may not always call close on the response body. Rails depends on the response body being closed in order for its CurrentAttributes implementation to work correctly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Information Disclosure Vulnerability (GHSA-rmj8-8hhh-gv5h) - Wind.
↪..`
OID:1.3.6.1.4.1.25623.1.0.147673
Version used: `2022-02-24T03:03:30Z`

References

```
cve: CVE-2022-23634
url: https://github.com/advisories/GHSA-rmj8-8hhh-gv5h
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0625
dfn-cert: DFN-CERT-2022-1898
dfn-cert: DFN-CERT-2022-1891
dfn-cert: DFN-CERT-2022-1506
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1195
dfn-cert: DFN-CERT-2022-1187
dfn-cert: DFN-CERT-2022-0992

Medium (CVSS: 5.3)

NVT: Ruby on Rails Active Record Security Bypass Vulnerability (Jan 2016) - Windows

Summary
Ruby on Rails is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 4.1.14.1
Installation
path / port: /

Impact
Successful exploitation will allow a remote attacker to bypass intended change restrictions by leveraging use of the nested attributes feature.

Solution:
Solution type: VendorFix
Update to version 3.2.22.1, 4.1.14.1, 4.2.5.1 or later.

Affected Software/OS
Ruby on Rails before 3.1.x and 3.2.x before 3.2.22.1, Ruby on Rails 4.0.x and 4.1.x before 4.1.14.1 and Ruby on Rails 4.2.x before 4.2.5.1 on Windows.

Vulnerability Insight
The flaw is due to the script 'activerecord/lib/active_record/nested_attributes.rb' does not properly implement a certain destroy option.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Active Record Security Bypass Vulnerability (Jan 2016) - Windows
OID:1.3.6.1.4.1.25623.1.0.809358

... continues on next page ...

... continued from previous page ...

Version used: 2025-09-09T05:38:49Z

References

```
cve: CVE-2015-7577
url: http://www.openwall.com/lists/oss-security/2016/01/25/10
url: http://www.securityfocus.com/bid/81806
cert-bund: WID-SEC-2025-1085
cert-bund: CB-K17/0278
cert-bund: CB-K16/0625
cert-bund: CB-K16/0419
cert-bund: CB-K16/0254
cert-bund: CB-K16/0166
cert-bund: CB-K16/0165
dfn-cert: DFN-CERT-2017-0284
dfn-cert: DFN-CERT-2016-0674
dfn-cert: DFN-CERT-2016-0458
dfn-cert: DFN-CERT-2016-0272
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2016-0178
```

Medium (CVSS: 5.3)

NVT: Ruby on Rails Active Model Security Bypass Vulnerability (Jan 2016) - Windows

Summary

Ruby on Rails is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 4.1.1
Fixed version:     4.1.14.1
Installation
path / port:       /
```

Impact

Successful exploitation will allow a remote attacker to bypass intended change restrictions by leveraging use of the nested attributes feature.

Solution:

Solution type: VendorFix

Update to version 4.1.14.1, 4.2.5.1 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Ruby on Rails 4.1.x before 4.1.14.1, Ruby on Rails 4.2.x before 4.2.5.1 on Windows.

Vulnerability Insight
The flaw is due to Ruby on Rails supports the use of instance-level writers for class accessors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Active Model Security Bypass Vulnerability (Jan 2016) - Windows`
OID:1.3.6.1.4.1.25623.1.0.809360
Version used: `2025-09-09T05:38:49Z`

References
`cve: CVE-2016-0753`
`url: http://www.openwall.com/lists/oss-security/2016/01/25/14`
`url: http://www.securityfocus.com/bid/82247`
`cert-bund: WID-SEC-2025-1085`
`cert-bund: CB-K16/0625`
`cert-bund: CB-K16/0254`
`cert-bund: CB-K16/0238`
`cert-bund: CB-K16/0236`
`cert-bund: CB-K16/0166`
`cert-bund: CB-K16/0165`
`dfn-cert: DFN-CERT-2016-0674`
`dfn-cert: DFN-CERT-2016-0272`
`dfn-cert: DFN-CERT-2016-0259`
`dfn-cert: DFN-CERT-2016-0258`
`dfn-cert: DFN-CERT-2016-0181`
`dfn-cert: DFN-CERT-2016-0178`

Medium (CVSS: 5.3)

NVT: Ruby on Rails Action View 'render' Directory Traversal Vulnerability (Feb 2016) - Windows

Summary
Ruby on Rails is prone to a directory traversal vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 4.1.1
Fixed version:     4.1.14.2
Installation
path / port:       /
```

Impact

... continues on next page ...

... continued from previous page ...

Successful exploitation will allow a remote attacker to read arbitrary files by leveraging an application's unrestricted use of the render method.

Solution:
Solution type: VendorFix
Update to version 3.2.22.2, 4.1.14.2 or later.

Affected Software/OS
Ruby on Rails versions before 3.2.22.2 and 4.x before 4.1.14.2 on Windows.

Vulnerability Insight
The flaw is due to an improper validation of crafted requests to action view, one of the components of action pack.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Ruby on Rails Action View 'render' Directory Traversal Vulnerability (Feb 2016).`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.809354
Version used: `2025-09-09T05:38:49Z`

References
`cve: CVE-2016-2097`
`url: https://www.debian.org/security/2016/dsa-3509`
`url: http://www.securityfocus.com/bid/83726`
`url: https://groups.google.com/g/rubyonrails-security/c/ddY6HgqB2z4/m/we0RasMZIA`
`↪AJ`
`cert-bund: WID-SEC-2022-2271`
`cert-bund: CB-K16/0522`
`cert-bund: CB-K16/0419`
`cert-bund: CB-K16/0372`
`dfn-cert: DFN-CERT-2022-2796`
`dfn-cert: DFN-CERT-2016-0566`
`dfn-cert: DFN-CERT-2016-0458`
`dfn-cert: DFN-CERT-2016-0404`

Medium (CVSS: 5.0)

NVT: Ruby on Rails Active Support DoS Vulnerability (Jun 2015) - Windows

Summary
Ruby on Rails is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 4.1.11
Installation
path / port: /

Impact
Successful exploitation will allow a remote attacker to cause denial of service attack.

Solution:
Solution type: VendorFix
Update to version 4.1.11, 4.2.2 or later.

Affected Software/OS
Ruby on Rails before 4.1.11 and Ruby on Rails 4.2.x before 4.2.2 on Windows.

Vulnerability Insight
The flaw is due to Specially crafted XML documents can cause applications to raise a SystemStackError and potentially cause a denial of service attack.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails Active Support DoS Vulnerability (Jun 2015) - Windows
OID:1.3.6.1.4.1.25623.1.0.807383
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2015-3227
url: http://openwall.com/lists/oss-security/2015/06/16/16
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/bahr2J
↪Lnxvk/x4EocXnHPp8J
cert-bund: CB-K16/0166
cert-bund: CB-K15/1056
cert-bund: CB-K15/0856
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2015-1111
dfn-cert: DFN-CERT-2015-0899

Medium (CVSS: 4.3)

NVT: Ruby on Rails Active Support XSS Vulnerability (Jun 2015) - Windows

Summary
Ruby on Rails is prone to a cross-site scripting (XSS) vulnerability.

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 4.1.1
Fixed version:     4.1.11
Installation
path / port:       /
```

Impact

Successful exploitation will allow a remote attacker to inject arbitrary web script or HTML via crafted parameters.

Solution:

Solution type: VendorFix

Update to version 4.2.2, 4.1.11 or later.

Affected Software/OS

Ruby on Rails versions 3.x, 3.0.x, 3.1.x, 3.2.x, 4.1.x before 4.1.11, 4.2.x before 4.2.2 on Linux.

Vulnerability Insight

The flaw is due to error in handling 'ActiveSupport::JSON.encode' method which can lead to an XSS attack.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: `Ruby on Rails Active Support XSS Vulnerability (Jun 2015) - Windows`

OID:1.3.6.1.4.1.25623.1.0.807381

Version used: `2025-09-09T05:38:49Z`

References

```
cve: CVE-2015-3226
url: http://openwall.com/lists/oss-security/2015/06/16/17
url: https://groups.google.com/forum/message/raw?msg=rubyonrails-security/7VlB_p
↪ck3hU/3QZrGIaQW6cJ
cert-bund: CB-K16/0166
cert-bund: CB-K15/0856
dfn-cert: DFN-CERT-2016-0181
dfn-cert: DFN-CERT-2015-0899
```

Medium (CVSS: 4.3)

NVT: Ruby on Rails < 5.2.5, 6.x < 6.0.4 CSRF Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

Ruby on Rails is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 4.1.1
Fixed version: 5.2.5
Installation
path / port: /

Impact
Successful exploitation would allow an authenticated attacer to perform actions in the context of another user.

Solution:
Solution type: VendorFix
Update to version 5.2.5, 6.0.4 or later.

Affected Software/OS
Ruby on Rails through version 5.2.4 and versions 6.0.0 through 6.0.3.

Vulnerability Insight
An attacker can use a global CSRF token, as can be found in the authenticity_token meta tag, to forge form-specific CSRF tokens.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Ruby on Rails < 5.2.5, 6.x < 6.0.4 CSRF Vulnerability
OID:1.3.6.1.4.1.25623.1.0.113714
Version used: 2025-09-09T05:38:49Z

References
cve: CVE-2020-8166
url: https://hackerone.com/reports/732415
cert-bund: WID-SEC-2023-1093
cert-bund: CB-K20/0477
dfn-cert: DFN-CERT-2024-0110
dfn-cert: DFN-CERT-2021-0842
dfn-cert: DFN-CERT-2020-2327
dfn-cert: DFN-CERT-2020-2093

[return to 10.0.0.31]

2.1.13 Medium 9200/tcp

Medium (CVSS: 6.8)

NVT: Elastic Elastisearch < 1.2 RCE Vulnerability - Active Check

Summary
Elastic Elasticsearch is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
`Vulnerable URL: http://10.0.0.31:9200/_search?source=%7B%22size%22%3A1%2C%22quer`
`↪y%22%3A%7B%22filtered%22%3A%7B%22query%22%3A%7B%22match_all%22%3A%7B%7D%7D%7D%`
`↪7D%2C%22script_fields%22%3A%7B%22VTTest%22%3A%7B%22script%22%3A%22import%20jav`
`↪a.util.*%3B%5Cnimport%20java.io.*%3B%5Cnnew%20Scanner(new%20File(%5C%22%2Fwind`
`↪ows%2Fwin.ini%5C%22)).useDelimiter(%5C%22%5C%5C%5C%5CZ%5C%22).next()%3B%22%7D%`
`↪7D%7D&callback=?`

Impact
An attacker can exploit this issue to execute arbitrary code.

Solution:
Solution type: VendorFix
Update to version 1.2 or later which disables 'dynamic scripting' by default. If the system was already updated make sure that this option is kept disabled.

Affected Software/OS
Elastic Elasticsearch versions prior to 1.2.

Vulnerability Insight
Elastic Elasticsearch has a flaw in its default configuration which makes it possible for any webpage to execute arbitrary code on visitors with Elasticsearch installed.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `Elastic Elastisearch < 1.2 RCE Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105032
Version used: `2025-09-03T08:26:15Z`

References
`cve: CVE-2014-3120`
`url: https://bou.ke/blog/elasticsearch-rce/`
`url: https://www.elastic.co/blog/found-elasticsearch-security#staying-safe-while`
`↪-developing-with-elasticsearch`
`url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog`
`cisa: Known Exploited Vulnerability (KEV) catalog`
`cert-bund: CB-K14/1131`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2014-1188

Medium (CVSS: 6.5)

NVT: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)

Summary
Elasticsearch is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 1.1.1
Fixed version: 6.8.17
Installation
path / port: /

Solution:
Solution type: VendorFix
Update to version 6.8.17, 7.13.3 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.17 and 7.x prior to 7.13.3.

Vulnerability Insight
An uncontrolled recursion vulnerability that could lead to a denial of service attack was identified in the Elasticsearch Grok parser. A user with the ability to submit arbitrary queries to Elasticsearch could create a malicious Grok query that will crash the Elasticsearch node.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Elastic Elasticsearch DoS Vulnerability (ESA-2021-15)
OID:1.3.6.1.4.1.25623.1.0.146386
Version used: 2025-09-03T08:26:15Z

References
cve: CVE-2021-22144
url: https://discuss.elastic.co/t/elasticsearch-7-13-3-and-6-8-17-security-updat
↪e/278100
cert-bund: WID-SEC-2022-1777
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2022-2315

Medium (CVSS: 6.5)

NVT: Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerability - Windows

Summary
Elasticsearch is prone to a field disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.12
Installation
path / port:       /
```

Impact
An attacker could gain additional permissions against a restricted index.

Solution:
Solution type: VendorFix
Update to version 6.8.12, 7.9.1 or later.

Affected Software/OS
Elasticsearch prior to version 6.8.12 and 7.9.0.

Vulnerability Insight
A field disclosure flaw was found in Elasticsearch when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.12, 7.x < 7.9.0 Information Disclosure Vulnerabilit.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.144431
Version used: `2025-09-03T08:26:15Z`

References
```
cve: CVE-2020-7019
url: https://discuss.elastic.co/t/elastic-stack-7-9-0-and-6-8-12-security-update
↪/245456
```

Medium (CVSS: 5.9)

NVT: Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability (ESA-2019-07) - Windows

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.2
Installation
path / port:       /
```

Impact
On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

Solution:
Solution type: VendorFix
Update to version 6.8.2 or 7.2.1 respectively.

Affected Software/OS
Elasticsearch through version 6.8.1 and version 7.0.0 through 7.2.0.

Vulnerability Insight
A race condition flaw was found in the response headers Elasticsearch returns to a request.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch < 6.8.2, 7.x < 7.2.1 Information Disclosure Vulnerability. ↪..`
OID:1.3.6.1.4.1.25623.1.0.117162
Version used: `2025-09-03T08:26:15Z`

References
```
cve: CVE-2019-7614
url: https://discuss.elastic.co/t/elastic-stack-6-8-2-and-7-2-1-security-update/
↪192963
url: https://www.elastic.co/community/security/
cert-bund: WID-SEC-2024-3184
```

Medium (CVSS: 5.3)

NVT: Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)

Summary
Elasticsearch is prone to multiple vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.15
Installation
path / port:       /
```

Impact
This could lead to disclosing the existence of documents and fields the attacker should not be able to view or result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.15, 7.12.0 or later.

Affected Software/OS
Elasticsearch versions prior to versions 6.8.15 or 7.12.0.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-22135: Suggester & Profile API information disclosure flaw
- CVE-2021-22137: Field disclosure flaw

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Multiple Vulnerabilities (ESA-2021-06, ESA-2021-08)`
OID:1.3.6.1.4.1.25623.1.0.145940
Version used: `2025-09-03T08:26:15Z`

References
```
cve: CVE-2021-22135
cve: CVE-2021-22137
url: https://discuss.elastic.co/t/elastic-stack-7-12-0-and-6-8-15-security-updat
↪e/268125
cert-bund: WID-SEC-2022-0720
dfn-cert: DFN-CERT-2025-0933
```

Medium (CVSS: 4.9)

NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.14
Installation
path / port:       /
```

Impact
This could allow an Elasticsearch administrator to view sensitive details.

Solution:
Solution type: VendorFix
Update to version 6.8.14, 7.10.0 or later.

Affected Software/OS
Elasticsearch versions prior to 6.8.14 and 7.0.0 prior to 7.10.0.

Vulnerability Insight
Elasticsearch has an information disclosure issue when audit logging and the emit_request_body option is enabled. The Elasticsearch audit log could contain sensitive information such as password hashes or authentication tokens.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2021-03)`
OID:1.3.6.1.4.1.25623.1.0.145383
Version used: `2025-09-03T08:26:15Z`

References
```
cve: CVE-2020-7021
url: https://discuss.elastic.co/t/elastic-stack-7-11-0-and-6-8-14-security-updat
↪e/263915
url: https://www.elastic.co/community/security
dfn-cert: DFN-CERT-2025-0933
```

Medium (CVSS: 4.3)

NVT: Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows

Summary
Elasticsearch is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 1.1.1`
`Fixed version: 1.4.0.Beta1`

Impact
Successful exploitation will allow remote attackers to inject arbitrary web script or HTML.

Solution:
Solution type: VendorFix
Update to Elasticsearch version 1.4.0.Beta1, or later.

Affected Software/OS
Elasticsearch version 1.3.x and prior on Windows.

Vulnerability Insight
The Flaw is due to an error in the CORS functionality.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elasticsearch Cross-site Scripting (XSS) Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.808092
Version used: `2025-09-03T08:26:15Z`

References
`cve: CVE-2014-6439`
`url: https://www.elastic.co/community/security/`
`url: http://www.securityfocus.com/bid/70233`
`url: http://www.securityfocus.com/archive/1/archive/1/533602/100/0/threaded`

[return to 10.0.0.31]

2.1.14 Medium 8022/tcp

Medium (CVSS: 6.1)

NVT: ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities

Summary
ManageEngine Desktop Central is prone to multiple cross-site scripting (XSS) vulnerabilities.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw allows to inject client-side script into Desktop Centrals web page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.812576
Version used: `2022-04-13T07:21:45Z`

References
```
cve: CVE-2018-8722
url: https://www.manageengine.com/products/desktop-central/cross-site-scripting-
↪vulnerability.html
url: http://www.securityfocus.com/bid/103426
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://10.0.0.31:8022/configurations.do:j_password`

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

Medium (CVSS: 4.3)

NVT: ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability

Summary
ManageEngine Desktop Central is prone to a reflected cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 9.1.084
Fixed version:     9.2.026
Installation
path / port:       /
```

Impact
Successful exploitation will allow attacker to cause cross site scripting and steal the cookie of other active sessions.

Solution:
Solution type: VendorFix
Update to version 9.2.026 or later.

Affected Software/OS
ManageEngine Desktop Central version 9.1.099 and prior.

Vulnerability Insight
The flaw exists as input passed via 'To' parameter of 'Specify Delivery Format' is not validated properly.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `ManageEngine Desktop Central <= 9.1.099 Reflected XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.807741
Version used: `2021-09-23T03:58:52Z`

References
`url: https://packetstormsecurity.com/files/136463`

[return to 10.0.0.31]

2.1.15 Medium 135/tcp

Medium (CVSS: 5.0)

NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49154]
     Annotation: XactSrv service
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49154]
     Annotation: Impl friendly name
Port: 49158/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.31[49158]
     Named pipe : lsass
```

... continues on next page ...

... continued from previous page ...

```
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49179/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:10.0.0.31[49179]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[return to 10.0.0.31]

2.1.16 Medium 21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Password required for anonymous.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 10.0.0.31]

2.1.17 Medium 22/tcp

Medium (CVSS: 5.3)

NVT: OpenSSH < 7.6 'sftp-server' Security Bypass Vulnerability - Windows

Product detection result
`cpe:/a:openbsd:openssh:7.1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

Summary
OpenSSH is prone to a security bypass vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 7.1
Fixed version:     7.6
Installation
path / port:       22/tcp
```

Impact
Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:
Solution type: VendorFix
Update to version 7.6 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSH versions prior to 7.6 on Windows.

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.6 'sftp-server' Security Bypass Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: `2024-12-13T05:05:32Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2017-15906`
`url: https://www.openssh.com/txt/release-7.6`
`url: http://www.securityfocus.com/bid/101552`
`url: https://github.com/openbsd/src/commit/a6981567e8e`
`cert-bund: WID-SEC-2024-1082`
`cert-bund: CB-K20/0041`
`cert-bund: CB-K18/0137`
`cert-bund: CB-K17/2126`
`cert-bund: CB-K17/2014`
`cert-bund: CB-K17/2002`
`dfn-cert: DFN-CERT-2024-1260`
`dfn-cert: DFN-CERT-2019-0362`
`dfn-cert: DFN-CERT-2018-2554`
`dfn-cert: DFN-CERT-2018-2191`
`dfn-cert: DFN-CERT-2018-2068`
`dfn-cert: DFN-CERT-2018-1828`
`dfn-cert: DFN-CERT-2018-1568`
`dfn-cert: DFN-CERT-2018-0150`
`dfn-cert: DFN-CERT-2017-2217`
`dfn-cert: DFN-CERT-2017-2100`
`dfn-cert: DFN-CERT-2017-2093`

Medium (CVSS: 5.3)

NVT: OpenSSH < 7.8 User Enumeration Vulnerability - Windows

Product detection result
`cpe:/a:openbsd:openssh:7.1`
`Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)`

Summary
OpenSSH is prone to a user enumeration vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 7.1`
`Fixed version: 7.8`
`Installation path / port: 22/tcp`

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution:
Solution type: VendorFix
Update to version 7.8 or later.

Affected Software/OS
OpenSSH versions 7.7 and prior.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH < 7.8 User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `2023-07-20T05:05:18Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.108577)

References

```
cve: CVE-2018-15473
url: https://0day.city/cve-2018-15473.html
url: https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d
↪1e0
cert-bund: WID-SEC-2024-1082
cert-bund: CB-K20/0041
cert-bund: CB-K18/1031
cert-bund: CB-K18/0873
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2021-2178
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-0228
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-0857
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2018-2293
dfn-cert: DFN-CERT-2018-2259
dfn-cert: DFN-CERT-2018-2191
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1696
```

Medium (CVSS: 5.3)

NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows

Product detection result

```
cpe:/a:openbsd:openssh:7.1
Detected by OpenSSH Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.108577)
```

Summary

OpenSSH is prone to a user enumeration vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 7.1
Fixed version:     None
Installation
path / port:       22/tcp
```

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
OpenSSH version 5.9 through 7.8.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Windows`
OID:1.3.6.1.4.1.25623.1.0.813887
Version used: `2021-05-28T07:06:21Z`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.1`
Method: `OpenSSH Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.108577)

References
`cve: CVE-2018-15919`
`url: https://bugzilla.novell.com/show_bug.cgi?id=1106163`
`url: https://seclists.org/oss-sec/2018/q3/180`
`cert-bund: WID-SEC-2024-1082`
`cert-bund: CB-K18/0885`
`dfn-cert: DFN-CERT-2024-1260`
`dfn-cert: DFN-CERT-2018-2293`
`dfn-cert: DFN-CERT-2018-2191`

[return to 10.0.0.31]

2.1.18 Low 9200/tcp

Low (CVSS: 3.1)

NVT: Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)

Summary
Elasticsearch is prone to an information disclosure vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.1.1
Fixed version:     6.8.13
Installation
path / port:       /
```

Impact
This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.

Solution:
Solution type: VendorFix
Update to version 6.8.13, 7.9.2 or later.

Affected Software/OS
Elasticsearch versions before 6.8.13 and 7.x before 7.9.2.

Vulnerability Insight
A document disclosure flaw was found in Elasticsearch when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Elastic Elasticsearch Information Disclosure Vulnerability (ESA-2020-13)`
OID:1.3.6.1.4.1.25623.1.0.117181
Version used: `2025-09-03T08:26:15Z`

References
```
cve: CVE-2020-7020
url: https://discuss.elastic.co/t/elastic-stack-7-9-3-and-6-8-13-security-update
↪/253033
url: https://www.elastic.co/community/security
cert-bund: WID-SEC-2022-0607
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2022-1530
```

[return to 10.0.0.31]

2.1.19 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 592259
Packet 2: 592366
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

... continues on next page ...

... continued from previous page ...

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 10.0.0.31]

2.1.20 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:

... continues on next page ...

. . . continued from previous page . . .

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 10.0.0.31]