



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

[Sponsor](#)

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

Scan Information ([show all](#)):

- dependency-check version: 12.1.0
- Report Generated On: Fri, 22 Aug 2025 18:45:38 -0400
- Dependencies Scanned: 49 (36 unique)
- Vulnerable Dependencies: 21
- Vulnerabilities Found: 212
- Vulnerabilities Suppressed: 0
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:hibernate:hibernate-validator:6.0.18:***:***:*** cpe:2.3:a:redhat:hibernate_validator:6.0.18:***:***:***	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	3	Highest
jackson-core-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:***:***:***	pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2	HIGH	2	Low
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:***:***:*** cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:***:***:***	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest
json-path-2.4.0.jar	cpe:2.3:a:json-path:jayway_jsonpath:2.4.0:***:***:***	pkg:maven/com.jayway.jsonpath/json-path@2.4.0	MEDIUM	1	Highest
json-smart-2.3.jar	cpe:2.3:a:json-smart_project:json-smart:2.3:***:***:*** cpe:2.3:a:json-smart_project:json-smart-v2:2.3:***:***:***	pkg:maven/net.minidev/json-smart@2.3	HIGH	3	Highest
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:***:***:***	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1	Highest
logback-classic-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:***:***:***	pkg:maven/ch.qos.logback/logback-classic@1.2.3	HIGH	2	Highest
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:***:***:***	pkg:maven/ch.qos.logback/logback-core@1.2.3	HIGH	4	Highest
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:***:***:***	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	8	Highest
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:***:***:***	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	CRITICAL	3	Highest
spring-boot-starter-web-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:***:***:*** cpe:2.3:a:web_project:web:2.2.4:release:***:***:***	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE	CRITICAL	3	Highest
spring-context-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***:***	pkg:maven/org.springframework/spring-context@5.2.3.RELEASE	CRITICAL*	13	Highest
spring-core-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***:***	pkg:maven/org.springframework/spring-core@5.2.3.RELEASE	CRITICAL*	13	Highest
spring-data-rest-webmvc-3.2.4.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_data_rest:3.2.4:release:***:***:*** cpe:2.3:a:vmware:spring_data_rest:3.2.4:release:***:***:***	pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE	MEDIUM	2	Highest
spring-expression-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***:***	pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE	CRITICAL*	13	Highest
spring-hateoas-1.0.3.RELEASE.jar	cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:***:***:***	pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE	MEDIUM	1	Highest
spring-tx-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***:*** cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***:***	pkg:maven/org.springframework/spring-tx@5.2.3.RELEASE	CRITICAL*	12	Highest

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:springsource:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:vmware:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:web_project:web:5.2.3:release:***.*.*.*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	CRITICAL*	18	Highest
spring-webmvc-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:springsource:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:vmware:spring_framework:5.2.3:release:***.*.*.* cpe:2.3:a:web_project:web:5.2.3:release:***.*.*.*	pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE	CRITICAL*	13	Highest
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:***.*.*.* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:***.*.*.*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL*	45	Highest
tomcat-embed-websocket-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:***.*.*.* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:***.*.*.*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30	CRITICAL*	46	Highest

* indicates the dependency has a known exploited vulnerability

Dependencies (vulnerable)

hibernate-validator-6.0.18.Final.jar

Description:

Hibernate's Bean Validation (JSR-380) reference implementation.

License:

<http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar\m2\repository\org\hibernate\validator\hibernate-validator\6.0.18.Final\hibernate-validator-6.0.18.Final.jar

MD5: d3eeb4f1bf013d939b86dfc34b0c6a5d

SHA1: 7fd00bcd87e14b6ba66279282ef15efa30dd2492

SHA256: 79fb11445bc48e1ea6fb259e825d58b3c9a5fa2b7e3c9527e41e4aeda82de907

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

- [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](#) (Confidence:High)
- [cpe:2.3:a:hibernate:hibernate-validator:6.0.18:***.*.*.*](#) (Confidence:Highest) [suppress](#)
- [cpe:2.3:a:redhat:hibernate_validator:6.0.18:***.*.*.*](#) (Confidence:Highest) [suppress](#)

Published Vulnerabilities

[CVE-2025-35036 \(OSSINDEX\)](#) [suppress](#)

Hibernate Validator before 6.2.0 and 7.0.0, by default and depending how it is used, may interpolate user-supplied input in a constraint violation message with Expression Language. This could allow an attacker to access sensitive information or execute arbitrary Java code. Hibernate Validator as of 6.2.0 and 7.0.0 no longer interpolates custom constraint violation messages with Expression Language and strongly recommends not allowing user-supplied input in constraint violation messages. CVE-2020-5245 and CVE-2025-4428 are examples of related, downstream vulnerabilities involving Expression Language interpolation of user-supplied data.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv2:

- Base Score: MEDIUM (6.900000095367432)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:L/I:L/V:A:L/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-35036\] CWE-94: Improper Control of Generation of Code \('Code Injection'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-35036>
- OSSIndex - https://docs.jboss.org/hibernate/stable/validator/reference/en-US/html_single/#section-hibernateconstraintvalidatorcontext
- OSSIndex - <https://github.com/advisories/GHSA-7v6m-28jr-rg84>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.hibernate.validator:hibernate-validator:6.0.18.Final:***.*.*.*

[CVE-2023-1932](#) [suppress](#)

A flaw was found in hibernate-validator's 'isValid' method in the org.hibernate.validator.internal.constraintvalidators.hv.SafeHtmlValidator class, which can be bypassed by omitting the tag ending in a less-than character. Browsers may render an invalid html, allowing HTML injection or Cross-Site-Scripting (XSS) attacks.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-1932\] CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)

- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1932>
- OSSIndex - <https://github.com/advisories/GHSA-x83m-pf6f-pf9g>
- secalert@redhat.com - [ISSUE TRACKING.VENDOR ADVISORY](#)
- secalert@redhat.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:hibernate:hibernate-validator:.*:.*:.*:.*:.* versions up to \(excluding\) 6.2](#)
- ...

[CVE-2020-10693](#) suppress

A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.

CWE-20 Improper Input Validation

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- OSSINDEX - [\[CVE-2020-10693\] CWE-20: Improper Input Validation](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693>
- OSSIndex - <https://github.com/hibernate/hibernate-validator/pull/1092>
- OSSIndex - <https://github.com/hibernate/hibernate-validator/pull/1093>
- OSSIndex - <https://github.com/hibernate/hibernate-validator/pull/1094>
- OSSIndex - <https://hibernate.atlassian.net/browse/HV-1774>
- OSSIndex - <https://in.relation.to/2020/05/07/hibernate-validator-615-6020-released/>
- OSSIndex - <https://openliberty.io/docs/latest/security-vulnerabilities.html>
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE TRACKING THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- secalert@redhat.com - [ISSUE TRACKING THIRD PARTY ADVISORY](#)
- secalert@redhat.com - [PATCH THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:redhat:hibernate_validator:.*:.*:.*:.*:.* versions from \(including\) 5.0.0; versions up to \(excluding\) 6.0.20](#)
- ...

jackson-core-2.10.2.jar

Description:

Core Jackson processing abstractions (aka Streaming API), implementation for JSON

License:

<http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar\l.m2\repository\com\fasterxml\jackson\core\jackson-core\2.10.2\jackson-core-2.10.2.jar

MD5: 5514a46e38331f8c8262ea63bf36483e

SHA1: 73d4322a6bda684f676a2b5fe918361c4e5c7cca

SHA256:4c41f22a48f6ebb28752baeb6d25bf09ba4ff0ad8fb82650dde448928b9da4f

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE

Evidence

Identifiers

- [pkg:maven/com.fasterxml.jackson.core:jackson-core@2.10.2](#) (Confidence:High)
- [cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:.*:.*:.*:.*](#) (Confidence:Low) suppress

Published Vulnerabilities

[CVE-2025-52999](#) suppress

jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. In versions prior to 2.15.0, if a user parses an input file and it has deeply nested data, Jackson could end up throwing a StackOverflowError if the depth is particularly large. jackson-core 2.15.0 contains a configurable limit for how deep Jackson will traverse in an input document, defaulting to an allowable depth of 1000. jackson-core will throw a StreamConstraintsException if the limit is reached. jackson-databind also benefits from this change because it uses jackson-core to parse JSON inputs. As a workaround, users should avoid parsing input files from untrusted sources.

CWE-121 Stack-based Buffer Overflow

CVSSv2:

- Base Score: HIGH (8.699999809265137)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:N/I:N/V:A:H/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-52999\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-52999>
- OSSIndex - <https://github.com/FasterXML/jackson-core/security/advisories/GHSA-h46c-h94j-95f3>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:com.fasterxml.jackson.core:jackson-core:2.10.2:.*:.*:.*:.*:*

CVE-2025-49128 (OSSINDEX) suppress

Jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. Starting in version 2.0.0 and prior to version 2.13.0, a flaw in jackson-core's `JsonLocation._appendSourceDesc` method allows up to 500 bytes of unintended memory content to be included in exception messages. When parsing JSON from a byte array with an offset and length, the exception message incorrectly reads from the beginning of the array instead of the logical payload start. This results in possible information disclosure in systems using pooled or reused buffers, like Netty or Vert.x. This issue was silently fixed in jackson-core version 2.13.0, released on September 30, 2021, via PR #652. All users should upgrade to version 2.13.0 or later. If upgrading is not immediately possible, applications can mitigate the issue by disabling exception message exposure to clients to avoid returning parsing exception messages in HTTP responses and/or disabling source inclusion in exceptions to prevent Jackson from embedding any source content in exception messages, avoiding leakage.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2025-49128> for details

CWE-209 Generation of Error Message Containing Sensitive Information

CVSSv2:

- Base Score: MEDIUM (6.900000095367432)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-49128\] CWE-209: Information Exposure Through an Error Message](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49128>
- OSSIndex - <https://github.com/FasterXML/jackson-core/security/advisories/GHSA-wf8f-6423-gfxg>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:com.fasterxml.jackson.core:jackson-core:2.10.2:.*:.*:.*:.*:*

jackson-databind-2.10.2.jar**Description:**

General data-binding functionality for Jackson: works on core streaming API

License:

<http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar1.m2\repository\com\fasterxml\jackson\core\jackson-databind\2.10.2\jackson-databind-2.10.2.jar

MD5: 057751b4e2dd1104be8caad6e9a3e589

SHA1: 0528de95f198afafbcfb0c09d2e43b6e0ea663ec

SHA256: 42c25644e35fadfbbed1b7f35a8d1e70a86737f190e43aa2c56cea4b96cbda88

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/com.fasterxml.jackson.core:jackson-databind@2.10.2](#) (Confidence:High)
- [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:.*:.*:.*:.*:*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:.*:.*:.*:*](#) (Confidence:Low) suppress

Published Vulnerabilities**CVE-2020-25649** suppress

A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

CWE-611 Improper Restriction of XML External Entity Reference

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- OSSINDEX - [\[CVE-2020-25649\] CWE-611: Improper Restriction of XML External Entity Reference \('XXE'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649>
- OSSIndex - <https://github.com/FasterXML/jackson-databind/issues/2589>

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:fasterxml:jackson-databind:2.10.0_2.10.5.1](#) versions from (including) 2.10.0, versions up to (excluding) 2.10.5.1
 - ...

[CVE-2020-36518](#) suppress

jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.

CWE-787 Out-of-bounds Write

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
 - Vector: /AV:N/AC:I /Au:N/C:N/I:N/A:P

References

- OSSINDEX - [CVE-2020-36518] [CWE-787: Out-of-bounds Write](#)
 - OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518>
 - OSSIndex - <https://github.com/FasterXML/jackson-databind/issues/2816>
 - af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_MAILING_LIST_THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING_THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISEDY](#)
 - cve@mitre.org - [EXPLOIT_MAILING_LIST_THIRD_PARTY ADVISEDY](#)
 - cve@mitre.org - [ISSUE_TRACKING_THIRD_PARTY ADVISEDY](#)
 - cve@mitre.org - [MAILING_LIST_THIRD_PARTY ADVISEDY](#)
 - cve@mitre.org - [THIRD_PARTY ADVISEDY](#)

Vulnerable Software & Versions: (show all)

- [cpe:2.3:a:fasterxml:jackson-databind:***.*.*.*](#) versions up to (excluding) 2.12.6.1
 - ...

CVE-2021-46877 suppress

jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to cause a denial of service (2 GB transient heap usage per read) in uncommon situations involving JsonNode JDK serialization.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/L:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2021-46877\]](#)
 - OSSIndex - <https://github.com/FasterXML/jackson-databind/issues/3328>
 - af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT ISSUE TRACKING VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST RELEASE NOTES](#)
 - cve@mitre.org - [EXPLOIT ISSUE TRACKING VENDOR ADVISORY](#)
 - cve@mitre.org - [MAILING LIST RELEASE NOTES](#)

Vulnerable Software & Versions: (show all)

- [cpe:2.3:a:fasterxml:jackson-databind:.*.*.*.*.*](#) versions from (including) 2.10.0; versions up to (excluding) 2.12.6
 -

[CVE-2022-42003](#)

In FasterXML jackson-databind before versions 2.13.4.1 and 2.12.17.1, resource exhaustion can occur because of a lack of a check in primitive value deserializers to avoid deep wrapper array nesting, when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/LU:N/S:U/C:N/I:N/A:H/E:3.9/PC:B/MAV:A

References

- OSSINDEX - [\[CVE-2022-42003\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42003>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:fasterxml:jackson-databind:.*:.*:.*:.*:.*](#) versions up to (excluding) 2.12.7.1
- ...

[CVE-2022-42004](#) suppress

In FasterXML jackson-databind before 2.13.4, resource exhaustion can occur because of a lack of a check in BeanDeserializer._deserializeFromArray to prevent use of deeply nested arrays. An application is vulnerable only with certain customized choices for deserialization.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-42004\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42004>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490>
- OSSIndex - <https://github.com/FasterXML/jackson-databind/issues/3582>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:fasterxml:jackson-databind:.*:.*:.*:.*:.*](#) versions up to (excluding) 2.12.7.1
- ...

[CVE-2023-35116](#) suppress

jackson-databind through 2.15.2 allows attackers to cause a denial of service or other unspecified impact via a crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that this is not a valid vulnerability report, because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (4.7)
- Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.0/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING](#)
- cve@mitre.org - [ISSUE_TRACKING](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:fasterxml:jackson-databind:.*:.*:.*:.*:.*](#) versions up to (excluding) 2.16.0

json-path-2.4.0.jar

Description:

Java port of Stefan Goessner JsonPath.

License:

The Apache Software License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar\.m2\repository\com\jayway\jsonpath\json-path\2.4.0\json-path-2.4.0.jar
MD5: 29169b4b1115bc851e5734ef35ecd42a
SHA1: 765a4401ceb2dc8d40553c2075eb80a8fa35c2ae
SHA256: 60441c74fb64e5a480070f86a604941927aaef684e2b513d780fb7a38fb4c5639
Referenced In Project/Scope: ssl-server:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-test@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/com.jayway.jsonpath/json-path@2.4.0](#) (Confidence:High)
- [cpe:2.3:a:com.jayway.jsonpath:2.4.0.*.*.*.*.*](#) (Confidence:Highest) [suppress](#)

Published Vulnerabilities[CVE-2023-51074 \(OSSINDEX\)](#) [suppress](#)

json-path v2.8.0 was discovered to contain a stack overflow via the Criteria.parse() method.

CWE-Other

CVSSv3:

- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

References:

- OSSINDEX - [\[CVE-2023-51074\] CWE-Other](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-51074>
- OSSIndex - <https://github.com/json-path/JsonPath/issues/973>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:com.jayway.jsonpath:json-path:2.4.0.*.*.*.*.*

json-smart-2.3.jar**Description:**

JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

License:

The Apache Software License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar\.m2\repository\net\minidev\json-smart\2.3\json-smart-2.3.jar

MD5: f2a921d4baaa7308de04eed4d8d72715

SHA1: 007396407491352ce4fa30de92efb158adb76b5b

SHA256: 903f48c8aa4c3f6426440b8d32de89fa1dc23b1169abde25e4e1d068aa67708b

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-test@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/net.minidev/json-smart@2.3](#) (Confidence:High)
- [cpe:2.3:a:net_minidev:json-smart:2.3.*.*.*.*.*](#) (Confidence:Highest) [suppress](#)
- [cpe:2.3:a:net_minidev:json-smart:2.3.*.*.*.*.*](#) (Confidence:Low) [suppress](#)

Published Vulnerabilities[CVE-2021-31684 \(OSSINDEX\)](#) [suppress](#)

A vulnerability was discovered in the indexOf function of JSONParserByteArray in JSON Smart versions 1.3 and 2.4 which causes a denial of service (DOS) via a crafted web request.

CWE-787 Out-of-bounds Write

CVSSv3:

- Base Score: HIGH (7.5)

- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:

- OSSINDEX - [\[CVE-2021-31684\] CWE-787: Out-of-bounds Write](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31684>
- OSSIndex - <https://github.com/netplex/json-smart-v1/issues/10>
- OSSIndex - <https://github.com/netplex/json-smart-v1/pull/11>
- OSSIndex - <https://github.com/netplex/json-smart-v2/issues/67>
- OSSIndex - <https://github.com/netplex/json-smart-v2/pull/68>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:.net:minidev:json-smart:2.3.*.*.*.*.*

CVE-2023-1370 suppress

[Json-smart](<https://netplex.github.io/json-smart/>) is a performance focused, JSON processor lib.

When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively.

It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software.

CWE-674 Uncontrolled Recursion

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-1370\] CWE-674: Uncontrolled Recursion](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-1370>
- OSSIndex - <https://ubuntu.com/security/CVE-2023-1370>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- reefs@jfrog.com - [EXPLOIT_THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:.json-smart_project:json-smart:*.**.*.*.*.* versions up to \(excluding\) 2.4.9](#)

CVE-2021-27568 suppress

An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.

CWE-754 Improper Check for Unusual or Exceptional Conditions

CVSSv3:

- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

References:

- OSSINDEX - [\[CVE-2021-27568\] CWE-754: Improper Check for Unusual or Exceptional Conditions](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27568>
- OSSIndex - <https://github.com/netplex/json-smart-v1/issues/7>
- OSSIndex - <https://github.com/netplex/json-smart-v1/pull/8>
- OSSIndex - <https://github.com/netplex/json-smart-v2/issues/60>
- OSSIndex - <https://github.com/netplex/json-smart-v2/pull/61>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [PATCH_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [PATCH_THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:.json-smart_project:json-smart-v2:*.**.*.*.*.* versions up to \(excluding\) 2.3.1](#)
- ...

log4j-api-2.12.1.jar**Description:**

The Apache Log4j API

License:

<https://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar.m2\repository\org\apache\logging\log4j\log4j-api\2.12.1\log4j-api-2.12.1.jar
MD5: 4a6f276d4fb426c8d489343c0325bb75
SHA1: a55e6d987f50a515c9260b0451b4fa217dc539cb

Published Vulnerabilities**CVE-2023-6378** suppress

A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-6378\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-6378>
- OSSIndex - <https://github.com/advisories/GHSA-vmq6-5m68-f53m>
- OSSIndex - <https://logback.qos.ch/news.html#1.3.12>
- af854a3a-2127-422b-91ae-364da2661108 - [RELEASE NOTES](#)
- vulnerability@ncsc.ch - [RELEASE NOTES](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:qos:logback:.*:.*:.*:.*:.* versions from \(including\) 1.2.0; versions up to \(excluding\) 1.2.13](#)
- ...

CVE-2021-42550 suppress

In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: MEDIUM (6.6)
- Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:0.7/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (8.5)
- Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

References:

- OSSINDEX - [\[CVE-2021-42550\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <https://jira.qos.ch/browse/LOGBACK-1591>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_ISSUE_TRACKING_PATCH_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- vulnerability@ncsc.ch - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:qos:logback:.*:.*:.*:.*:.* versions up to \(including\) 1.2.7](#)
- ...

logback-core-1.2.3.jar**Description:**

logback-core module

License:

<http://www.eclipse.org/legal/epl-v10.html>, <http://www.gnu.org/licenses/old-licenses/gpl-2.1.html>

File Path: C:\Users\leemar\m2\repository\ch\qos\logback\logback-core\1.2.3\logback-core-1.2.3.jar

MD5: 841fc00c6edff60d947a3872a2db4d45

SHA1: 86434400c3d4d92dfb0a305dc87d953677c03c

SHA256: 5946d837fe6f960c02a53eda7a6926ecc3c758bbdd69aa453ee429f858217f22

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/ch.qos.logback/logback-core@1.2.3](#) (Confidence:High)
- [cpe:2.3:a:qos:logback:1.2.3.*.*.*.*.*](#) (Confidence:Highest) [suppress]

Published Vulnerabilities

[CVE-2023-6378](#) [suppress]

A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-6378\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2023-6378>
- OSSIndex - <https://github.com/advisories/GHSA-vmq6-5m68-f53m>
- OSSIndex - <https://logback.qos.ch/news.html#1.3.12>
- af854a3a-2127-422b-91ae-364da2661108 - [RELEASE NOTES](#)
- vulnerability@ncsc.ch - [RELEASE NOTES](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:qos:logback:.*.*.*.*.*](#) versions from (including) [1.2.0](#); versions up to (excluding) [1.2.13](#)
- ...

[CVE-2021-42550](#) [suppress]

In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: MEDIUM (6.6)
- Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:0.7/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (8.5)
- Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

References:

- OSSINDEX - [\[CVE-2021-42550\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <https://jira.qos.ch/browse/LOGBACK-1591>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_ISSUE_TRACKING_PATCH_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- vulnerability@ncsc.ch - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [THIRD_PARTY_ADVISORY](#)
- vulnerability@ncsc.ch - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:qos:logback:.*.*.*.*.*](#) versions up to (including) [1.2.7](#)
- ...

[CVE-2024-12798 \(OSSINDEX\)](#) [suppress]

ACE vulnerability in JaninoEventEvaluator by QOS.CH logback-core upto including version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 in Java applications allows attacker to execute arbitrary code by compromising an existing logback configuration file or by injecting an environment variable before program execution.

Malicious logback configuration files can allow the attacker to execute arbitrary code using the JaninoEventEvaluator extension.

A successful attack requires the user to have write access to a configuration file. Alternatively, the attacker could inject a malicious environment variable pointing to a malicious configuration file. In both cases, the attack requires existing privilege.

CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv2:

- Base Score: MEDIUM (5.900000095367432)
- Vector: CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

References:

- OSSINDEX - [\[CVE-2024-12798\] CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement \('Expression Language Injection'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-12798>
- OSSIndex - <https://github.com/advisories/GHSA-pr98-23f8-jwxx>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:ch.qos.logback:logback-core:1.2.3.*.*.*.*.*

CVE-2024-12801 (OSSINDEX) suppress

Server-Side Request Forgery (SSRF) in SaxEventRecorder by QOS.CH logback version 0.1 to 1.3.14 and 1.4.0 to 1.5.12 on the Java platform, allows an attacker to forge requests by compromising logback configuration files in XML.

The attacks involves the modification of DOCTYPE declaration in XML configuration files.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2024-12801> for details

CWE-918 Server-Side Request Forgery (SSRF)

CVSSv2:

- Base Score: LOW (2.4000000953674316)
- Vector: CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:L/VI:N/VA:L/SC:H/SI:H/SA:H

References:

- OSSINDEX - [\[CVE-2024-12801\] CWE-918: Server-Side Request Forgery \(SSRF\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-12801>
- OSSIndex - <https://github.com/advisories/GHSA-6v67-2wr5-gv4>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:ch.qos.logback:logback-core:1.2.3.*.*.*.*.*

snakeyaml-1.25.jar**Description:**

YAML 1.1 parser and emitter for Java

License:

Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar\m2\repository\org\yaml\snakeyaml\1.25\snakeyaml-1.25.jar

MD5: 67d5b8f596047aae07a3bf6f23a0bf2

SHA1: 8b6e01ef61d8378ae6dd7b511a7f2a33fae1421

SHA256: b50ef33187e7dc922b26dbe4dd0fdb3a9cf349e75a08b95269901548eee546eb

Referenced In Project/Scope: ssl-server:runtime

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/org.yaml/snakeyaml@1.25](#) (Confidence:High)
- [cpe:2.3:a:snakeyaml_project:snakeyaml:1.25.*.*.*.*.*](#) (Confidence:Highest) suppress

Published Vulnerabilities**CVE-2022-1471** suppress

SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConstructor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

CWE-502 Deserialization of Untrusted Data, CWE-20 Improper Input Validation

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-1471\] CWE-20: Improper Input Validation](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1471>
- OSSIndex - <https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, THIRD PARTY ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE TRACKING, THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT, THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT, THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT, THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [ISSUE TRACKING, THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*.*.*.*.*.* versions up to \(excluding\) 2.0](#)

[CVE-2017-18640](#) suppress

The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- OSSINDEX - [\[CVE-2017-18640\] CWE-776: Improper Restriction of Recursive Entity References in DTDs \('XML Entity Expansion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640>
- OSSIndex - <https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, ISSUE TRACKING, PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, ISSUE TRACKING, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [RELEASE NOTES, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- cve@mitre.org - [EXPLOIT, ISSUE TRACKING, PATCH, THIRD PARTY ADVISORY](#)
- cve@mitre.org - [EXPLOIT, ISSUE TRACKING, THIRD PARTY ADVISORY](#)
- cve@mitre.org - [PATCH, THIRD PARTY ADVISORY](#)
- cve@mitre.org - [RELEASE NOTES, THIRD PARTY ADVISORY](#)
- cve@mitre.org - [THIRD PARTY ADVISORY](#)
- cve@mitre.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*.*.*.*.*.* versions up to \(excluding\) 1.26](#)
- ...

[CVE-2022-25857](#) suppress

The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial of Service (DoS) due missing to nested depth limitation for collections.

CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-25857\] CWE-776: Improper Restriction of Recursive Entity References in DTDs \('XML Entity Expansion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-25857>
- OSSIndex - <https://bitbucket.org/snakeyaml/snakeyaml/issues/525>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, ISSUE TRACKING, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- report@snyk.io - [EXPLOIT, ISSUE TRACKING, THIRD PARTY ADVISORY](#)
- report@snyk.io - [EXPLOIT, PATCH, THIRD PARTY ADVISORY](#)
- report@snyk.io - [MAILING LIST, THIRD PARTY ADVISORY](#)
- report@snyk.io - [PATCH, THIRD PARTY ADVISORY](#)
- report@snyk.io - [PATCH, THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*.*.*.*.*.* versions up to \(excluding\) 1.31](#)

[CVE-2022-38749](#) suppress

Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.

CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-38749\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38749>
- OSSIndex - <https://bitbucket.org/snakeyaml/snakeyaml/issues/525>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47024>
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [MAILING LIST, THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [THIRD PARTY ADVISORY](#)

- cve-coordination@google.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*:.*:.*:.*:.* versions up to \(excluding\) 1.31](#)

[CVE-2022-38751](#)

Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.

CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-38751\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38751>
- OSSIndex - <https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039>
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [MAILING LIST THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*:.*:.*:.*:.* versions up to \(excluding\) 1.31](#)

[CVE-2022-38752](#)

Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack-overflow.

CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-38752\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38752>
- OSSIndex - <https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverflow-oss-fuzz-47081>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081>
- OSSIndex - <https://github.com/advisories/GHSA-9w3m-gqgf-c4p9>
- af854a3a-2127-422b-91ae-364da2661108 - [PERMISSIONS REQUIRED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [PERMISSIONS REQUIRED](#)
- cve-coordination@google.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*:.*:.*:.*:.* versions up to \(excluding\) 1.32](#)

[CVE-2022-41854](#)

Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack.

CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-41854\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41854>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT ISSUE TRACKING THIRD PARTY ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT ISSUE TRACKING THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*:.*:.*:.*:.* versions up to \(excluding\) 1.32](#)

[CVE-2022-38750](#)

Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow.

CWE-787 Out-of-bounds Write, CWE-121 Stack-based Buffer Overflow

CVSSv3:

- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:1.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2022-38750\] CWE-121: Stack-based Buffer Overflow](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38750>
- OSSIndex - <https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027>
- OSSIndex - <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027>

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT_ISSUE_TRACKING_MAILING_LIST_THIRD_PARTY_ADVISORY](#)
- cve-coordination@google.com - [EXPLOIT_ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve-coordination@google.com - [MAILING_LIST_THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:snakeyaml_project:snakeyaml:.*.*.*.*.* versions up to \(excluding\) 1.31](#)

spring-boot-2.2.4.RELEASE.jar**Description:**

Spring Boot

License:Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>**File Path:** C:\Users\leemar\m2\repository\org\springframework\boot\spring-boot\2.2.4.RELEASE\spring-boot-2.2.4.RELEASE.jar**MD5:** 24de0cfdb8ea74b903b562b43cbc5eb13**SHA1:** 225a4fd31156c254e3bb92adb42ee8c6de812714**SHA256:** 176befc7b90e8498f44e21994a70d69ba360ef1e858ff3cea8282e802372daf2**Referenced In Project/Scope:** ssl-server:compile**Included by:** pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE**Evidence****Related Dependencies****Identifiers**

- [pkg:maven/org.springframework.boot:spring-boot@2.2.4.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:vmware:spring_boot:2.2.4:release.*.*.*.*](#) (Confidence:Highest) [suppress]

Published Vulnerabilities[CVE-2023-20873](#) [suppress]

In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

NVD-CWE-noinfo

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_boot:.*.*.*.*.* versions up to \(excluding\) 2.5.15](#)
- ...

[CVE-2022-27772](#) [suppress]

spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer

CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- OSSINDEX - [\[CVE-2022-27772\] CWE-668: Exposure of Resource to Wrong Sphere](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772>
- OSSIndex - <https://github.com/JLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85>

- OSSIndex - <https://github.com/github/codeql/pull/4473#issuecomment-1030416237>
- OSSIndex - <https://github.com/spring-projects/spring-boot/issues/23622>
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,PATCH,THIRD PARTY ADVISORY](#)
- cve@mitre.org - [EXPLOIT,PATCH,THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:vmware:spring_boot:*.**.*.*.* versions up to \(excluding\) 2.2.11](#)

[CVE-2023-20883](#) [suppress](#)

In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_boot:*.**.*.*.* versions up to \(excluding\) 2.5.14](#)
- ...

spring-boot-starter-web-2.2.4.RELEASE.jar**Description:**

Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

File Path: C:\Users\leemar.l.m2\repository\org\springframework\boot\spring-boot-starter-web\2.2.4.RELEASE\spring-boot-starter-web-2.2.4.RELEASE.jar

MD5: 0fd2927b6235bdbaa0d4d12c28a847c2

SHA1: ec75d01d212b5229c16d872f2b127744c0ed46ed8

SHA256: eb4d4ad19fe1724fd02cfce9c467c0b67766b5a4a54d0e54fc51826d9e3d87b8

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/com.snhu/ssl-server@0.0.1-SNAPSHOT

Evidence**Identifiers**

- [pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:vmware:spring_boot:2.2.4:release:*.**.*.*](#) (Confidence:Highest) [suppress](#)
- [cpe:2.3:a:web_project:web:2.2.4:release:*.**.*.*](#) (Confidence:Highest) [suppress](#)

Published Vulnerabilities[CVE-2023-20873](#) [suppress](#)

In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

NVD-CWE-noinfo

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_boot:*.**.*.*.* versions up to \(excluding\) 2.5.15](#)
- ...

[CVE-2022-27772](#) [suppress](#)

spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer

CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,PATCH,THIRD_PARTY ADVISEDY](#)
- cve@mitre.org - [EXPLOIT,PATCH,THIRD_PARTY ADVISEDY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:vmware:spring_boot:***.*.*.*.* versions up to \(excluding\) 2.2.11](#)

[CVE-2023-20883](#) suppress

In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISEDY](#)
- security@vmware.com - [VENDOR ADVISEDY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_boot:***.*.*.*.* versions up to \(excluding\) 2.5.14](#)
- ...

spring-context-5.2.3.RELEASE.jar

Description:

Spring Context

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

File Path: C:\Users\leemar.m2\repository\org\springframework\spring-context\5.2.3.RELEASE\spring-context-5.2.3.RELEASE.jar

MD5: a5ba542a35f3c9fc630df1715ccf325

SHA1: 7750c95c96c7a1885c8b1b503ba915bc33ca579a

SHA256:82c625cffed80685b153700359a6c6d5c91018069a0171cf21a7defb0267e993

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

- [pkg:maven/org.springframework.spring-context@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:springsource:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:vmware:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) suppress

Published Vulnerabilities

[CVE-2022-22965](#) suppress

CISA Known Exploited Vulnerability:

- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit.

However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,THIRD PARTY ADVISORY,VDB ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [US GOVERNMENT RESOURCE](#)
- security@vmware.com - [EXPLOIT,THIRD PARTY ADVISORY,VDB ENTRY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:***:*** versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2024-22259](#) suppress

Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

This is the same as CVE-2024-22243 <https://spring.io/security/cve-2024-22243>, but with different input.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:***:*** versions up to \(excluding\) 5.3.33](#)
- ...

[CVE-2021-22118](#) suppress

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:***:*** versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.15](#)
- ...

- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

[CVE-2023-20863](#) suppress

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

[CVE-2022-22968](#) suppress

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- OSSINDEX - [\[CVE-2022-22968\] CWE-178: Improper Handling of Case Sensitivity](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/28333>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/28334>
- OSSIndex - <https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2022-22968>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

[CVE-2022-22970](#) suppress

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

[CVE-2021-22060](#) suppress

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.*: versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

[CVE-2021-22096](#) suppress

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.*: versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

[CVE-2025-22233 \(OSSINDEX\)](#) suppress

CVE-2024-38820 ensured Locale-independent, lowercase conversion for both the configured disallowedFields patterns and for request parameter names. However, there are still cases where it is possible to bypass the disallowedFields checks.

Affected Spring Products and Versions

Spring Framework:

- * 6.2.0 - 6.2.6
- * 6.1.0 - 6.1.19
- * 6.0.0 - 6.0.27
- * 5.3.0 - 5.3.42
- * Older, unsupported versions are also affected

Mitigation

Users of affected versions should upgrade to the corresponding fixed version.

Affected version(s) Fix Version Availability 6.2.x

6.2.7

OSS6.1.x

6.1.20

OSS6.0.x

6.0.28

Commercial <https://enterprise.spring.io/> 5.3.x

5.3.43

Commercial <https://enterprise.spring.io/>

No further mitigation steps are necessary.

Generally, we recommend using a dedicated model object with properties only for data binding, or using constructor binding since constructor arguments explicitly declare what to bind together with turning off setter binding through the declarativeBinding flag. See the Model Design section in the reference documentation.

For setting binding, prefer the use of allowedFields (an explicit list) over disallowedFields.

Credit

This issue was responsibly reported by the TERASOLUNA Framework Development Team from NTT DATA Group Corporation.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2025-22233> for details

CWE-20 Improper Input Validation

CVSSv2:

- Base Score: LOW (2.299999952316284)
- Vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/V/A:N/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-22233\] CWE-20: Improper Input Validation](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-22233>
- OSSIndex - <https://spring.io/security/cve-2025-22233>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-context:5.2.3.RELEASE:***:***:*

spring-core-5.2.3.RELEASE.jar

Description:

Spring Core

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>**File Path:** C:\Users\leemar.m2\repository\org\springframework\spring-core\5.2.3.RELEASE\spring-core-5.2.3.RELEASE.jar**MD5:** ae11e44d9eff630186b9e095e70b59de**SHA1:** 3734223040040e8c3fecc5faa3ae8a1ed6da146b**SHA256:** 6df908f4deaeefdb03b56a00246cc0dc0d941d9636e811025bcfc5a2a44851**Referenced In Project/Scope:** ssl-server:compile**Included by:** pkg:maven/org.springframework.boot/spring-boot-starter-test@2.2.4.RELEASE

Evidence

Identifiers

- [pkg:maven/org.springframework:spring-core@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***:*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***:*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***:*](#) (Confidence:Highest) [suppress]

Published Vulnerabilities

CVE-2022-22965 [suppress]

CISA Known Exploited Vulnerability:

- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [US_GOVERNMENT_RESOURCE](#)
- security@vmware.com - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)

- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY VDB ENTRY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:5.2.0](#) versions up to (excluding) 5.2.20
- ...

[CVE-2025-41242 \(OSSINDEX\)](#) suppress

Spring Framework MVC applications can be vulnerable to a "Path Traversal Vulnerability" when deployed on a non-compliant Servlet container.

An application can be vulnerable when all the following are true:

- * the application is deployed as a WAR or with an embedded Servlet container
- * the Servlet container does not reject suspicious sequences <https://jakarta.ee/specifications/servlet/6.1/jakarta-servlet-spec-6.1.html#uri-path-canonicalization>
- * the application serves static resources <https://docs.spring.io/spring-framework/reference/web/webmvc/mvc-config/static-resources.html#page-title> with Spring resource handling

We have verified that applications deployed on Apache Tomcat or Eclipse Jetty are not vulnerable, as long as default security features are not disabled in the configuration. Because we cannot check exploits against all Servlet containers and configuration variants, we strongly recommend upgrading your application.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2025-41242> for details

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:

- Base Score: HIGH (8.199999809265137)
- Vector: CVSS:4.0/AV:N/AC:L/PR:N/UI:N/VC:H/V:I/N/VA:N/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-41242\] CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-41242>
- OSSIndex - <https://spring.io/security/cve-2025-41242>

Vulnerable Software & Versions (OSSINDEX):

- [cpe:2.3:a:org.springframework:spring-core:5.2.3.RELEASE](#)

[CVE-2024-22259](#) suppress

Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

This is the same as CVE-2024-22243 <https://spring.io/security/cve-2024-22243>, but with different input.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:5.3.0](#) versions up to (excluding) 5.3.33
- ...

[CVE-2021-22118](#) suppress

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.15](#)
- ...

[CVE-2020-5421](#)

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [NOT_APPLICABLE_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@pivotal.io - [NOT_APPLICABLE_THIRD_PARTY_ADVISORY](#)
- security@pivotal.io - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@pivotal.io - [THIRD_PARTY_ADVISORY](#)
- security@pivotal.io - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.9](#)
- ...

[CVE-2022-22950](#)

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2022-22971](#)

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.21](#)
- ...

[CVE-2023-20861](#)

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

CVE-2023-20863 [suppress](#)

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

CVE-2022-22968 [suppress](#)

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

CVE-2022-22970 [suppress](#)

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

CVE-2021-22060 [suppress](#)

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

[CVE-2021-22096](#) suppress

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

spring-data-rest-webmvc-3.2.4.RELEASE.jar

Description:

Spring Data REST - WebMVC

File Path: C:\Users\leemar.lm2\repository\org\springframework\data\spring-data-rest-webmvc\3.2.4.RELEASE\spring-data-rest-webmvc-3.2.4.RELEASE.jar

MD5: da22f3d4eb417e9e0a7ae9a73961c4f0

SHA1: acaae431117245ed5f1d09166207b076bbe3ac82

SHA256: 7694c509ffaff229d45630d2ee68525588f80d2740deef7642696f1440043d1

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE

Evidence

Identifiers

- [pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_data_rest:3.2.4:release:***.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:vmware:spring_data_rest:3.2.4:release:***.*.*.*](#) (Confidence:Highest) suppress

Published Vulnerabilities

[CVE-2021-22047 \(OSSINDEX\)](#) suppress

In Spring Data REST versions 3.4.0 - 3.4.13, 3.5.0 - 3.5.5, and older unsupported versions, HTTP resources implemented by custom controllers using a configured base API path and a controller type-level request mapping are additionally exposed under URLs that can potentially be exposed for unauthorized access depending on the Spring Security configuration.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: MEDIUM (5.30000190734863)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:

- OSSINDEX - [\[CVE-2021-22047\] CWE-200: Information Exposure](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22047>
- OSSIndex - <https://github.com/spring-projects/spring-data-rest/issues/1342>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2021-22047>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework.data:spring-data-rest-webmvc:3.2.4.RELEASE:.*.*.*.*.*

[CVE-2022-31679 \(OSSINDEX\)](#) suppress

Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6.0 - 3.5.5, 3.7.0 - 3.7.2, and older unsupported versions, if an attacker knows about the structure of the underlying domain model, they can craft HTTP requests that expose hidden entity attributes.

CWE-noinfo

CVSSv3:

- Base Score: LOW (3.700000047683716)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:

- OSSINDEX - [\[CVE-2022-31679\] CWE-noinfo](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-31679>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2022-31679>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework.data:spring-data-rest-webmvc:3.2.4.RELEASE:.*.*.*.*.*

spring-expression-5.2.3.RELEASE.jar**Description:**

Spring Expression Language (SpEL)

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

File Path: C:\Users\leemar\.m2\repository\org\springframework\spring-expression\5.2.3.RELEASE\spring-expression-5.2.3.RELEASE.jar

MD5: f2d2fe04f9fb9c23b03d07839393de5a

SHA1: d0c6bb10758805b2153c589686b8045554bfac2d

SHA256: 1ba798e1f4da9e5ad68e67d7e7abe39f141674762c8755d952edeb0380d384b9

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/org.springframework.spring-expression@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:.*.*.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:springsource:spring_framework:5.2.3:release:.*.*.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:vmware:spring_framework:5.2.3:release:.*.*.*.*.*](#) (Confidence:Highest) suppress

Published Vulnerabilities[CVE-2022-22965](#) suppress**CISA Known Exploited Vulnerability:**

- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT, THIRD PARTY ADVISORY, VDB ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION, VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY, VDB ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [US GOVERNMENT RESOURCE](#)
- security@vmware.com - [EXPLOIT, THIRD PARTY ADVISORY, VDB ENTRY](#)
- security@vmware.com - [MITIGATION, VENDOR ADVISORY](#)
- security@vmware.com - [PATCH, THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH, THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY, VDB ENTRY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:*** versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2024-22259](#) suppress

Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

This is the same as CVE-2024-22243 <https://spring.io/security/cve-2024-22243>, but with different input.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:*** versions up to \(excluding\) 5.3.33](#)
- ...

[CVE-2021-22118](#) suppress

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH, THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:*** versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.15](#)
- ...

[CVE-2020-5421](#) suppress

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:/P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [NOT_APPLICABLE THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@pivotal.io - [NOT_APPLICABLE THIRD PARTY ADVISORY](#)
- security@pivotal.io - [PATCH THIRD PARTY ADVISORY](#)
- security@pivotal.io - [THIRD PARTY ADVISORY](#)
- security@pivotal.io - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.9](#)
- ...

[CVE-2022-22950](#) suppress

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- OSSINDEX - [\[CVE-2022-22950\] CWE-770: Allocation of Resources Without Limits or Throttling](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/28145>
- OSSIndex - <https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2022-22950>
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION VENDOR ADVISORY](#)
- security@vmware.com - [MITIGATION VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2022-22971](#) suppress

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION VENDOR ADVISORY](#)
- security@vmware.com - [PATCH THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.21](#)
- ...

[CVE-2023-20861](#) suppress

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-20861\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861>
- OSSIndex - <https://spring.io/blog/2023/03/20/spring-framework-5-2-23-fixes-cve-2023-20861>

- OSSIndex - <https://spring.io/security/cve-2023-20861>
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

[CVE-2023-20863](#) suppress

In spring framework versions prior to 5.2.24 release+ , 5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-20863\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/30325>
- OSSIndex - <https://spring.io/security/cve-2023-20863>
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

[CVE-2024-38808 \(OSSINDEX\)](#) suppress

In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) expression that may cause a denial of service (DoS) condition.

Specifically, an application is vulnerable when the following is true:

- The application evaluates user-supplied SpEL expressions.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2024-38808> for details

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:

- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/V/C:N/VI:N/VA:L/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2024-38808\] CWE-770: Allocation of Resources Without Limits or Throttling](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38808>
- OSSIndex - <https://spring.io/security/cve-2024-38808>

Vulnerable Software & Versions (OSSINDEX):

- [cpe:2.3:a:org.springframework:spring-expression:5.2.3.RELEASE:***.*.*.*](#)

[CVE-2022-22968](#) suppress

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

[CVE-2022-22970](#) suppress

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)

- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
- CVSSv2:
- Base Score: LOW (3.5)
 - Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

[CVE-2021-22060](#) suppress

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

[CVE-2021-22096](#) suppress

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

spring-hateoas-1.0.3.RELEASE.jar**Description:**

Library to support implementing representations for hyper-text driven REST web services.

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

File Path: C:\Users\leemar.m2\repository\org\springframework\hateoas\spring-hateoas\1.0.3.RELEASE\spring-hateoas-1.0.3.RELEASE.jar

MD5: efbd177ffbc4a8c7a693080528c9cd8

SHA1: 35c3514a8336d31f34677b5c99de2f1fe32611ac

SHA256: 5a54edfd6ae2e6a85bd694682a358a0a55282f426623da59d47d879de3e1846d

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:***:***](#) (Confidence:Highest) [suppress]

Published Vulnerabilities[CVE-2023-34036](#) [suppress]

Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server.

For the application to be affected, it needs to satisfy the following requirements:

- * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses.
- * The application infrastructure does not guard against clients submitting (X-)Forwarded... headers.

CWE-644 Improper Neutralization of HTTP Headers for Scripting Syntax, CWE-116 Improper Encoding or Escaping of Output

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-34036\] CWE-116: Improper Encoding or Escaping of Output](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-34036>
- OSSIndex - <https://github.com/advisories/GHSA-7m5c-fgwf-mwph>
- OSSIndex - <https://spring.io/security/cve-2023-34036>
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_hateoas:***:***:***:*** versions up to \(excluding\) 1.5.5](#)
- ...

spring-tx-5.2.3.RELEASE.jar**Description:**

Spring Transaction

License:

Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

File Path: C:\Users\leemar.m2\repository\org\springframework\spring-tx\5.2.3.RELEASE\spring-tx-5.2.3.RELEASE.jar

MD5: fab4ecac70d561ceb80c755aed804081

SHA1: 99acf44c9844accb84f88672d273ff01527a9592

SHA256: ecaad16431f612082f1b8724e45294ed4eee24346acd1a33fb3939018aff60b7

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-data-rest@2.2.4.RELEASE

Evidence**Related Dependencies****Identifiers**

- [pkg:maven/org.springframework.spring-tx@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***:***](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:springsource:spring_framework:5.2.3:release:***:***](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:vmware:spring_framework:5.2.3:release:***:***](#) (Confidence:Highest) [suppress]

Published Vulnerabilities

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.15](#)
- ...

[CVE-2020-5421](#) suppress

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [NOT_APPLICABLE,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@pivotal.io - [NOT_APPLICABLE,THIRD PARTY ADVISORY](#)
- security@pivotal.io - [PATCH,THIRD PARTY ADVISORY](#)
- security@pivotal.io - [THIRD PARTY ADVISORY](#)
- security@pivotal.io - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.9](#)
- ...

[CVE-2022-22950](#) suppress

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- OSSINDEX - [\[CVE-2022-22950\] CWE-770: Allocation of Resources Without Limits or Throttling](#)
- OSSIndex - [http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950](#)
- OSSIndex - [https://github.com/spring-projects/spring-framework/issues/28145](#)
- OSSIndex - [https://spring.io/blog/2022/03/17/spring-framework-6.0-0-m3-and-5.3-17-available-now](#)
- OSSIndex - [https://tanzu.vmware.com/security/cve-2022-22950](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2022-22971](#) suppress

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION, VENDOR ADVISORY](#)
- security@vmware.com - [PATCH, THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.21](#)
- ...

[CVE-2023-20861](#) suppress

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-20861\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861>
- OSSIIndex - <https://spring.io/blog/2023/03/20/spring-framework-5-2-23-fixes-cve-2023-20861>
- OSSIIndex - <https://spring.io/security/cve-2023-20861>
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

[CVE-2023-20863](#) suppress

In spring framework versions prior to 5.2.24 release+, 5.3.27+ and 6.0.8+, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2023-20863\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863>
- OSSIIndex - <https://github.com/spring-projects/spring-framework/issues/30325>
- OSSIIndex - <https://spring.io/security/cve-2023-20863>
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

[CVE-2022-22968](#) suppress

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

[CVE-2022-22970](#) suppress

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)

- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A
- CVSSv2:
- Base Score: LOW (3.5)
 - Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

[CVE-2021-22060](#) suppress

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

[CVE-2021-22096](#) suppress

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

spring-web-5.2.3.RELEASE.jar**Description:**

Spring Web

License:Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>**File Path:** C:\Users\leemar.m2\repository\org\springframework\spring-web\5.2.3.RELEASE\spring-web-5.2.3.RELEASE.jar**MD5:** a89d6690cd14159a6ac1e875e54411**SHA1:** dd386a02e40b915ab400a3bf9f586d2dc4c0852c**SHA256:** 25d264969c624cb8103a7f2b36b148ea1be8b87780c4758e7f9a6e2bc8416d76**Referenced In Project/Scope:** ssl-server:compile**Included by:** pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE**Evidence**

Identifiers

- [pkg:maven/org.springframework/spring-web@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3;release:.*.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:springsource:spring_framework:5.2.3;release:.*.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:vmware:spring_framework:5.2.3;release:.*.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:web_project:web:5.2.3;release:.*.*.*.*](#) (Confidence:Highest) [suppress]

Published Vulnerabilities[CVE-2016-1000027](#) [suppress]

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- OSSINDEX - [\[CVE-2016-1000027\] CWE-502: Deserialization of Untrusted Data](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027>
- OSSIndex - <https://blog.gypryengineer.com/en/security/detecting-dangerous-spring-exporters-with-codeql.html>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/24434>
- OSSIndex - <https://www.tenable.com/security/research/tra-2016-20>
- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK_EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [RELEASE_NOTES_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [BROKEN_LINK_EXPLOIT_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [EXPLOIT_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [ISSUE_TRACKING_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [RELEASE_NOTES_THIRD_PARTY_ADVISORY](#)
- cve@mitre.org - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:vmware:spring_framework:.*.*.*.*](#) versions up to (excluding) 6.0.0

[CVE-2022-22965](#) [suppress]**CISA Known Exploited Vulnerability:**

- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [US_GOVERNMENT_RESOURCE](#)
- security@vmware.com - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)

- security@vmware.com - [PATCH THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY VDB ENTRY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:5.2.20](#) versions up to (excluding) 5.2.20
- ...

CVE-2024-38809 (OSSINDEX) [suppress](#)

Applications that parse ETags from "If-Match" or "If-None-Match" request headers are vulnerable to DoS attack.

Users of affected versions should upgrade to the corresponding fixed version.

Users of older, unsupported versions could enforce a size limit on "If-Match" and "If-None-Match" headers, e.g. through a Filter.

CWE-400 Uncontrolled Resource Consumption

CVSSv2:

- Base Score: HIGH (8.699999809265137)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/V:C:N/I:N/V:A:H/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2024-38809\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38809>
- OSSIndex - <https://spring.io/security/cve-2024-38809>

Vulnerable Software & Versions (OSSINDEX):

- [cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE](#)

CVE-2024-22243 (OSSINDEX) [suppress](#)

Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2024-22243> for details

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.100000381469727)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

References:

- OSSINDEX - [\[CVE-2024-22243\] CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22243>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/32211>
- OSSIndex - <https://spring.io/security/cve-2024-22243>

Vulnerable Software & Versions (OSSINDEX):

- [cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE](#)

CVE-2024-22262 (OSSINDEX) [suppress](#)

Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

This is the same as [CVE-2024-22259](#) <https://spring.io/security/cve-2024-22259> and [CVE-2024-22243](#) <https://spring.io/security/cve-2024-22243>, but with different input.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.100000381469727)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

References:

- OSSINDEX - [\[CVE-2024-22262\] CWE-601: URL Redirection to Untrusted Site \('Open Redirect'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22262>
- OSSIndex - <https://github.com/spring-projects/spring-framework/issues/32616>
- OSSIndex - <https://spring.io/security/cve-2024-22262>

Vulnerable Software & Versions (OSSINDEX):

- [cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE](#)

CVE-2024-22259 [suppress](#)

Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect <https://cwe.mitre.org/data/definitions/601.html> attack or to a SSRF attack if the URL is used after passing validation checks.

This is the same as [CVE-2024-22243](#) <https://spring.io/security/cve-2024-22243>, but with different input.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.3.33](#)
- ...

CVE-2021-22118 [suppress](#)

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

CWE-269 Improper Privilege Management, CWE-668 Exposure of Resource to Wrong Sphere

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

References:

- OSSINDEX - [\[CVE-2021-22118\] CWE-269: Improper Privilege Management](#)
- OSSIndex - [http://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2021-22118](#)
- OSSIndex - [https://github.com/spring-projects/spring-framework/issues/26931](#)
- OSSIndex - [https://tanzu.vmware.com/security/cve-2021-22118](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.15](#)
- ...

CVE-2025-41234 (OSSINDEX) [suppress](#)

Description

In Spring Framework, versions 6.0.x as of 6.0.5, versions 6.1.x and 6.2.x, an application is vulnerable to a reflected file download (RFD) attack when it sets a "Content-Disposition" header with a non-ASCII charset, where the filename attribute is derived from user-supplied input.

Specifically, an application is vulnerable when all the following are true:

- * The header is prepared with org.springframework.http.ContentDisposition.
- * The filename is set via ContentDisposition.Builder#filename(String, Charset).
- * The value for the filename is derived from user-supplied input.
- * The application does not sanitize the user-supplied input.
- * The downloaded content of the response is injected with malicious commands by the attacker (see RFD paper reference for details).

An application is not vulnerable if any of the following is true:

- * The application does not set a "Content-Disposition" response header.
- * The header is not prepared with org.springframework.http.ContentDisposition.
- * The filename is set via one of: * ContentDisposition.Builder#filename(String), or ContentDisposition.Builder#filename(String, ASCII)

- * The filename is not derived from user-supplied input.
- * The filename is derived from user-supplied input but sanitized by the application.
- * The attacker cannot inject malicious content in the downloaded content of the response.

Affected Spring Products and Versions

- * 6.2.0 - 6.2.7
- * 6.1.0 - 6.1.20
- * 6.0.5 - 6.0.28
- * Older, unsupported versions are not affected

Mitigation Users of affected versions should upgrade to the corresponding fixed version.

Affected version(s) Fix version Availability 6.2.x 6.2.8 OSS 6.1.x 6.1.21 OSS 6.0.x 6.0.29 Commercial https://enterprise.spring.io/ No further mitigation steps are necessary.

CWE-113 in 'Content-Disposition' handling in VMware Spring Framework versions 6.0.5 to 6.2.7 allows remote attackers to launch Reflected File Download (RFD) attacks via unsanitized user input in 'ContentDisposition.Builder#filename(String, Charset)' with non-ASCII charsets.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See <https://ossindex.sonatype.org/vulnerability/CVE-2025-41234> for details

CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')

CVSSv2:

- Base Score: HIGH (7.400000095367432)
- Vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:H/VI:H/V/A:N/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2025-41234\] CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers \('HTTP Response Splitting'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-41234>
- OSSIndex - <https://spring.io/security/cve-2025-41234>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:.*:.*:.*:.*

[CVE-2024-38828 \(OSSINDEX\)](#) suppress

Spring MVC controller methods with an @RequestBody byte[] method parameter are vulnerable to a DoS attack.

CWE-400 Uncontrolled Resource Consumption

CVSSv2:

- Base Score: MEDIUM (6.900000095367432)
- Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

References:

- OSSINDEX - [\[CVE-2024-38828\] CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion'\)](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38828>
- OSSIndex - <https://spring.io/blog/2024/11/15/spring-framework-cve-2024-38828-published>
- OSSIndex - <https://spring.io/security/cve-2024-38828>

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-web:5.2.3.RELEASE:.*:.*:.*:.*

[CVE-2020-5421](#) suppress

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N/E:1.3/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

References:

- OSSINDEX - [\[CVE-2020-5421\] CWE-noinfo](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2020-5421>
- af854a3a-2127-422b-91ae-364da2661108 - [NOT_APPLICABLE THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@pivotal.io - [NOT_APPLICABLE THIRD PARTY ADVISORY](#)
- security@pivotal.io - [PATCH THIRD PARTY ADVISORY](#)
- security@pivotal.io - [THIRD PARTY ADVISORY](#)
- security@pivotal.io - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:.*:.*:.*:.*:.* versions from \(including\) 5.2.0: versions up to \(excluding\) 5.2.9](#)
- ...

[CVE-2022-22950](#) suppress

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION VENDOR ADVISORY](#)
- security@vmware.com - [MITIGATION VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2022-22971](#)

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.21](#)
- ...

[CVE-2023-20861](#)

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

[CVE-2023-20863](#)

In spring framework versions prior to 5.2.24 release+, 5.3.27+ and 6.0.8+, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

[CVE-2022-22968](#)

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:.*.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

[CVE-2022-22970](#)

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H:E:1.6/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:.*.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

[CVE-2021-22060](#)

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:.*.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

[CVE-2021-22096](#)

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- OSSINDEX - [\[CVE-2021-22096\] CWE-117: Improper Output Neutralization for Logs](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2021-22096>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:.*.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

spring-webmvc-5.2.3.RELEASE.jar

Description:

Spring Web MVC

License:Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>**File Path:** C:\Users\leemar.m2\repository\org\springframework\spring-webmvc\5.2.3.RELEASE\spring-webmvc-5.2.3.RELEASE.jar**MD5:** 867cc7369d453637b5042ee4d6931a78**SHA1:** 745a62502023d2496b565b7fe102bb1ee229d6b7**SHA256:** b3b0a2477e67b050ddc08dc96e76db5950cbccba075e782c24f73eda49a0160**Referenced In Project/Scope:** ssl-server:compile**Included by:** pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE**Evidence****Identifiers**

- [pkg:maven/org.springframework.spring-webmvc@5.2.3.RELEASE](#) (Confidence:High)
- [cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:springsource:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:vmware:spring_framework:5.2.3:release:***.*.*.*](#) (Confidence:Highest) [suppress]
- [cpe:2.3:a:web_project:web:5.2.3:release:***.*.*.*](#) (Confidence:Highest) [suppress]

Published Vulnerabilities[CVE-2022-22965](#) [suppress]**CISA Known Exploited Vulnerability:**

- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2022-22965>

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')**CVSSv3:**

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION_VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [US_GOVERNMENT_RESOURCE](#)
- security@vmware.com - [EXPLOIT_THIRD_PARTY_ADVISORY_VDB_ENTRY](#)
- security@vmware.com - [MITIGATION_VENDOR_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [PATCH_THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)
- security@vmware.com - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2024-38816 \(OSSINDEX\)](#) [suppress]

Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running.

Specifically, an application is vulnerable when both of the following are true:

- * the web application uses RouterFunctions to serve static resources
- * resource handling is explicitly configured with a FileSystemResource location

However, malicious requests are blocked and rejected when any of the following is true:

- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@pivotal.io - [NOT_APPLICABLE,THIRD PARTY ADVISORY](#)
- security@pivotal.io - [PATCH,THIRD PARTY ADVISORY](#)
- security@pivotal.io - [THIRD PARTY ADVISORY](#)
- security@pivotal.io - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.9](#)
- ...

[CVE-2022-22950](#) suppress

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(excluding\) 5.2.20](#)
- ...

[CVE-2022-22971](#) suppress

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.21](#)
- ...

[CVE-2023-20861](#) suppress

In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.22](#)
- ...

[CVE-2023-20863](#) suppress

In spring framework versions prior to 5.2.24 release+, 5.3.27+ and 6.0.8+, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

CWE-400 Uncontrolled Resource Consumption, CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(excluding\) 5.2.24](#)
- ...

[CVE-2022-22968](#) suppress

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions from \(including\) 5.2.0; versions up to \(including\) 5.2.20](#)
- ...

[CVE-2022-22970](#) suppress

In spring framework versions prior to 5.3.20+, 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:1.6/RC:R/MAV:A

CVSSv2:

- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MITIGATION,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [MITIGATION,VENDOR ADVISORY](#)
- security@vmware.com - [PATCH,THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***.*.*.*.* versions up to \(including\) 5.2.21](#)
- ...

[CVE-2021-22060](#) suppress

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- OSSINDEX - [\[CVE-2021-22060\] CWE-noinfo](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060>
- OSSIndex - <https://tanzu.vmware.com/security/cve-2021-22060>
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:***:*** versions from \(including\) 5.2.0; versions up to \(including\) 5.2.18](#)
- ...

CVE-2021-22096 suppress

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

CWE-117 Improper Output Neutralization for Logs, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [THIRD PARTY ADVISORY](#)
- security@vmware.com - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:vmware:spring_framework:***:***:***:*** versions from \(including\) 5.2.0; versions up to \(including\) 5.2.17](#)
- ...

tomcat-embed-core-9.0.30.jar**Description:**

Core Tomcat implementation

License:

Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar.m2\repository\org\apache\tomcat\embed\tomcat-embed-core\9.0.30\tomcat-embed-core-9.0.30.jar

MD5: f9e49f66756f133157f19e617af26ffe

SHA1: ad32909314fe2ba02cec036434c0addd19bcc580

SHA256: b1415eecbc9f14e3745c1bfd41512a1b8e1af1332a7bea4d4be30b2e0ba7b330

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](#) (Confidence:High)
- [cpe:2.3:a:apache:tomcat:9.0.30:***:***:***](#) (Confidence:Highest) suppress
- [cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:***:***:***](#) (Confidence:Highest) suppress

Published Vulnerabilities**CVE-2020-1938** suppress**CISA Known Exploited Vulnerability:**

- Product: Apache Tomcat
- Name: Apache Tomcat Improper Privilege Management Vulnerability
- Date Added: 2022-03-03
- Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-03-17
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2020-1938>

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

NVD-CWE-Other

CVSSv3:

- Base Score: CRITICAL (9.8)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
 - Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.31](#)
- ...

[CVE-2024-50379](#) [suppress](#)

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration).

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0-M1 through 9.0.97.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue.

CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.98](#)
- ...

[CVE-2024-52316](#) [suppress](#)

Unchecked Error Condition vulnerability in Apache Tomcat. If Tomcat is 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 fail, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100.

Users are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fix the issue.

CWE-754 Improper Check for Unusual or Exceptional Conditions, CWE-391 Unchecked Error Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.96](#)
- ...

[CVE-2024-56337](#) [suppress](#)

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0-M1 through 9.0.97.
The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

The mitigation for CVE-2024-50379 was incomplete.

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)

Tomcat 11.0.3, 10.1.35 and 9.0.99 onwards will include checks that sun.io.useCanonCaches is set appropriately before allowing the default servlet to be write enabled on a case insensitive file system. Tomcat will also set sun.io.useCanonCaches to false by default where it can.

CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.98](#)
- ...

[CVE-2025-24813](#) [suppress](#)

CISA Known Exploited Vulnerability:

- Product: Apache Tomcat
- Name: Apache Tomcat Path Equivalence Vulnerability
- Date Added: 2025-04-01
- Description: Apache Tomcat contains a path equivalence vulnerability that allows a remote attacker to execute code, disclose information, or inject malicious content via a partial PUT request.
- Required Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
- Due Date: 2025-04-22
- Notes: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: <https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkqg> ; <https://nvd.nist.gov/vuln/detail/CVE-2025-24813>

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0-M1 through 9.0.98.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that was 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 were true, a malicious user was able to perform remote code execution:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- application was using Tomcat's file based session persistence with the default storage location
- application included a library that may be leveraged in a deserialization attack

Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

CWE-44 Path Equivalence: 'file.name' (Internal Dot), CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE TRACKING](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions up to \(excluding\) 9.0.99](#)
- ...

[CVE-2025-31651](#) [suppress](#)

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. For a subset of unlikely rewrite rule configurations, it was possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.5, from 10.1.0-M1 through 10.1.39, from 9.0.0-M1 through 9.0.102.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.

CWE-116 Improper Encoding or Escaping of Output

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,RELEASE NOTES,VENDOR ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.1:9.0.36](#) versions from (including) 9.0.1; versions up to (including) 9.0.36
 - ...

[CVE-2020-13935](#) suppress

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

CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
 - Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

Vulnerable Software & Versions: (show all)

- [cpe:2.3:a:apache:tomcat:***:***:***:***](#) versions from (including) 9.0.1; versions up to (including) 9.0.36

[CVE-2020-17527](#) suppress

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

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/LI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

CVSSv3:

- Base Score: MEDIUM (5.0)
 - Vector: (/N/V/N/AG:L/A:/N/C:B//N/A:N)

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1: versions up to \(including\) 9.0.35](#)
- ...

[CVE-2021-25122](#) suppress

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0: versions up to \(including\) 9.0.41](#)
- ...

[CVE-2021-41079](#) suppress

Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

CWE-20 Improper Input Validation, CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.44](#)
- ...

[CVE-2022-29885](#) suppress

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

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
 - Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.MITIGATION.VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING_LIST.MITIGATION.VENDOR ADVISORY](#)
 - security@apache.org - [MAILING_LIST.THIRD_PARTY ADVISORY](#)
 - security@apache.org - [PATCH.THIRD_PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.13; versions up to \(including\) 9.0.62](#)
 -

[CVE-2022-42252](#) | [suppress](#)

If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting `rejectIllegalHeader` to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/LI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,VENDOR ADVISED](#)
 - security@apache.org - [MAILING_LIST,VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.0:9.0.68](#) versions from (including) 9.0.0; versions up to (excluding) 9.0.68

[CVE-2023-44487](#) | [Suppress](#)

CISA Known Exploited Vulnerability:

- A Known Exploited Vulnerability:**

 - Product: IETF HTTP/2
 - Name: HTTP/2 Rapid Reset Attack Vulnerability
 - Date Added: 2023-10-10
 - Description: HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).
 - Required Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
 - Due Date: 2023-10-31
 - Notes: This vulnerability affects a common open-source component, third-party library, or protocol used by different products. For more information, please see: [HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487 | CISA](https://www.cisa.gov/news-events/alerts/2023/10/10/htp2-rapid-reset-vulnerability-cve-2023-44487): <https://www.cisa.gov/news-events/alerts/2023/10/10/htp2-rapid-reset-vulnerability-cve-2023-44487>; <https://blog.cloudflare.com/technical-breakdown-htp2-rapid-reset-ddos-attack/>; <https://nvd.nist.gov/vuln/detail/CVE-2023-44487>

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

CWE-400 Uncontrolled Resource Consumption NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*****:***](#) versions from (including) 9.0.0; versions up to (including) 9.0.80
 - ...

[CVE-2023-46589](#) suppress

Improper Input Validation vulnerability in Apache Tomcat. Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M11 onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
 - security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)

- security@apache.org - [MAILING_LIST](#)[VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.83](#)
- ...

[CVE-2024-24549](#) suppress

Denial of Service due to improper input validation vulnerability for HTTP/2 requests in Apache Tomcat. When processing an HTTP/2 request, if the request exceeded any of the configured limits for headers, the associated HTTP/2 stream was not reset until after all of the headers had been processed. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

CWE-20 Improper Input Validation, NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)[THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@apache.org - [MAILING_LIST](#)
- security@apache.org - [MAILING_LIST](#)[THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.86](#)
- ...

[CVE-2024-34750](#) suppress

Improper Handling of Exceptional Conditions, Uncontrolled Resource Consumption vulnerability in Apache Tomcat. 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.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.0-M1 through 9.0.89.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100.

Users are recommended to upgrade to version 11.0.0-M21, 10.1.25 or 9.0.90, which fixes the issue.

CWE-400 Uncontrolled Resource Consumption, CWE-755 Improper Handling of Exceptional Conditions

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.90](#)
- ...

[CVE-2024-38286](#) suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.35 through 8.5.100 and 7.0.92 through 7.0.109.

Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue.

Apache Tomcat, under certain configurations on any platform, allows an attacker to cause an OutOfMemoryError by abusing the TLS handshake process.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.13; versions up to \(excluding\) 9.0.90](#)
- ...

[CVE-2025-48988](#)

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- OSSINDEX - [\[CVE-2025-48988\]](#) [CWE-770: Allocation of Resources Without Limits or Throttling](#)
- OSSIndex - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48988>
- OSSIndex - <https://github.com/advisories/GHSA-h3gc-fqg-6h8f>
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2025-48989](#)

Improper Resource Shutdown or Release vulnerability in Apache Tomcat made Tomcat vulnerable to the made you reset attack.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.9, from 10.1.0-M1 through 10.1.43 and from 9.0.0.M1 through 9.0.107. Older, EOL versions may also be affected.

Users are recommended to upgrade to one of versions 11.0.10, 10.1.44 or 9.0.108 which fix the issue.

CWE-404 Improper Resource Shutdown or Release

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.1; versions up to \(excluding\) 9.0.108](#)
- ...

[CVE-2025-49125](#)

Authentication Bypass Using an Alternate Path or Channel vulnerability in Apache Tomcat. When using PreResources or PostResources mounted other than at the root of the web application, it was possible to access those resources via an unexpected path. That path was likely not to be protected by the same security constraints as the expected path, allowing those security constraints to be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-288 Authentication Bypass Using an Alternate Path or Channel

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2025-52434](#)

Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Tomcat when using the APR/Native connector. This was particularly noticeable with client initiated closes of HTTP/2 connections.

This issue affects Apache Tomcat: from 9.0.0.M1 through 9.0.106. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 9.0.107, which fixes the issue.

CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [ISSUE TRACKING MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.107](#)

[CVE-2025-52520](#) suppress

For some unlikely configurations of multipart upload, an Integer Overflow vulnerability in Apache Tomcat could lead to a DoS via bypassing of size limits.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0-M1 through 9.0.106.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.

CWE-190 Integer Overflow or Wraparound

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [ISSUE TRACKING MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.107](#)
- ...

[CVE-2025-53506](#) suppress

Uncontrolled Resource Consumption vulnerability in Apache Tomcat if an HTTP/2 client did not acknowledge the initial settings frame that reduces the maximum permitted concurrent streams.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0-M1 through 9.0.106.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100.

Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [ISSUE TRACKING MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(including\) 9.0.106](#)
- ...

[CVE-2025-46701](#) suppress

Improper Handling of Case Sensitivity vulnerability in Apache Tomcat's GCI servlet allows security constraint bypass of security constraints that apply to the pathInfo component of a URI mapped to the CGI servlet.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.6, from 10.1.0-M1 through 10.1.40, from 9.0.0-M1 through 9.0.104.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.7, 10.1.41 or 9.0.105, which fixes the issue.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: HIGH (7.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.105](#)
- ...

[CVE-2020-9484](#) suppress

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

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.0)
 - Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.4)
 - Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

References:

Vulnerable Software & Versions: (show all)

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.1; versions up to \(excluding\) 9.0.43](#)
 -

CVE-2021-25329 suppress

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

NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.0)
 - Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.4)
 - Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)

- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0: versions up to \(including\) 9.0.41](#)
- ...

[CVE-2021-30640](#) suppress

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

CWE-116 Improper Encoding or Escaping of Output

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.46](#)
- ...

[CVE-2025-55668](#) suppress

Session Fixation vulnerability in Apache Tomcat via rewrite valve.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-384 Session Fixation

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:2.8/RC:R/MAV:A

References:

- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2024-23672](#) suppress

Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

CWE-459 Incomplete Cleanup

CVSSv3:

- Base Score: MEDIUM (6.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.86](#)
- ...

[CVE-2022-34305](#) suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.RELEASE_NOTES.THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST.RELEASE_NOTES.THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- security@apache.org - [THIRD_PARTY_ADVISORY](#)
- security@apache.org - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.30; versions up to \(including\) 9.0.64](#)
- ...

[CVE-2023-41080](#) suppress

URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. Older, EOL versions may also be affected.

The vulnerability is limited to the ROOT (default) web application.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE_TRACKING.PATCH.VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@apache.org - [ISSUE_TRACKING.PATCH.VENDOR_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(including\) 9.0.79](#)
- ...

[CVE-2021-24122](#) suppress

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CWE-706 Use of Incorrectly-Resolved Name or Reference, CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.VENDOR_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST.THIRD_PARTY_ADVISORY](#)
- security@apache.org - [MAILING_LIST.VENDOR_ADVISORY](#)
- security@apache.org - [THIRD_PARTY_ADVISORY](#)
- security@apache.org - [THIRD_PARTY_ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1; versions up to \(including\) 9.0.39](#)
- ...

[CVE-2021-33037](#) suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/I:U:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(excluding\) 9.0.0: versions up to \(including\) 9.0.46](#)
- ...

[CVE-2023-42795](#) [suppress](#)

Incomplete Cleanup vulnerability in Apache Tomcat. When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next. Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.

CWE-459 Incomplete Cleanup

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.81](#)
- ...

[CVE-2023-45648](#) [suppress](#)

Improper Input Validation vulnerability in Apache Tomcat. Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.

CWE-20 Improper Input Validation, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)

- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.81](#)
- ...

[CVE-2024-21733](#) suppress

Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43.

Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.

CWE-209 Generation of Error Message Containing Sensitive Information

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,PATCH,VENDOR ADVISORY](#)
- security@apache.org - [MAILING LIST,PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,PATCH,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.44](#)
- ...

[CVE-2024-54677](#) suppress

Uncontrolled Resource Consumption vulnerability in the examples web application provided with Apache Tomcat leads to denial of service.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0.M1 through 9.9.97.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*:*.** versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.98](#)
- ...

[CVE-2019-17569](#) suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.28; versions up to \(including\) 9.0.30](#)
- ...

CVE-2020-1935

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK_MAILING_LIST_THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_VENDOR ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- security@apache.org - [BROKEN_LINK_MAILING_LIST_THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST_VENDOR ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(including\) 9.0.30](#)
- ...

CVE-2020-13943

If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

NVD-CWE-noinfo

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH_THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISED](#)
- security@apache.org - [BROKEN_LINK](#)
- security@apache.org - [MAILING_LIST_THIRD_PARTY ADVISED](#)
- security@apache.org - [PATCH_THIRD_PARTY ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)
- security@apache.org - [VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.30:***:***:***](#)
- ...

CVE-2023-28708

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

Older, EOL versions may also be affected.

CWE-523 Unprotected Transport of Credentials

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,PATCH,VENDOR ADVISEDY](#)
- security@apache.org - [MAILING_LIST,PATCH,VENDOR ADVISEDY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*.*.* versions from \(excluding\) 9.0.0; versions up to \(excluding\) 9.0.72](#)
- ...

[CVE-2021-43980](#) suppress

The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an `Http1Processor` instance resulting in responses, or part responses, to be received by the wrong client.

CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CVSSv3:

- Base Score: LOW (3.7)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISEDY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISEDY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,VENDOR ADVISEDY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISEDY](#)
- security@apache.org - [MAILING_LIST,THIRD PARTY ADVISEDY](#)
- security@apache.org - [MAILING_LIST,THIRD PARTY ADVISEDY](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISEDY](#)
- security@apache.org - [THIRD PARTY ADVISEDY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*.**.*.*.* versions from \(including\) 9.0.0; versions up to \(including\) 9.0.60](#)
- ...

tomcat-embed-websocket-9.0.30.jar**Description:**

Core Tomcat implementation

License:

Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

File Path: C:\Users\leemar.m2\repository\org\apache\tomcat\embed\tomcat-embed-websocket\9.0.30\tomcat-embed-websocket-9.0.30.jar

MD5: 3b6e5bcc92cd9a6df4a17138ed4e011c

SHA1: 33157f6bc5bfd03380ebb5ac476db0600a04168d

SHA256: 4ce32add19b34a80376edb1e1678c373cb720c28c7a0d37a4361bf659c2ea84c

Referenced In Project/Scope: ssl-server:compile

Included by: pkg:maven/org.springframework.boot:spring-boot-starter-web@2.2.4.RELEASE

Evidence**Identifiers**

- [pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30](#) (Confidence:High)
- [cpe:2.3:a:apache:tomcat:9.0.30:*.**.*.*.*](#) (Confidence:Highest) suppress
- [cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*.**.*.*.*](#) (Confidence:Highest) suppress

Published Vulnerabilities[CVE-2020-1938](#) suppress**CISA Known Exploited Vulnerability:**

- Product: Apache Tomcat
- Name: Apache Tomcat Improper Privilege Management Vulnerability
- Date Added: 2022-03-03
- Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-03-17
- Notes: <https://nvd.nist.gov/vuln/detail/CVE-2020-1938>

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0-M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP

port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

NVD-CWE-Other

CVSSv3:

- Base Score: CRITICAL (9.8)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.5)
 - Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:

- security@apache.org - [MAILING_LIST.VENDOR ADVISORY](#)
- security@apache.org - [PATCH_THIRD_PARTY ADVISORY](#)
- security@apache.org - [PATCH_THIRD_PARTY ADVISORY](#)
- security@apache.org - [PATCH_THIRD_PARTY ADVISORY](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [RELEASE NOTES](#)
- security@apache.org - [THIRD_PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.31](#)
- ...

[CVE-2024-50379](#) suppress

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability during JSP compilation in Apache Tomcat permits an RCE on case insensitive file systems when the default servlet is enabled for write (non-default configuration).

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0-M1 through 9.0.97.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue.

CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST.VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.98](#)
- ...

[CVE-2024-52316](#) suppress

Unchecked Error Condition vulnerability in Apache Tomcat. If Tomcat is 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 fail, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100.

Users are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fix the issue.

CWE-754 Improper Check for Unusual or Exceptional Conditions, CWE-391 Unchecked Error Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST.VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.96](#)
- ...

[CVE-2024-56337](#) suppress

Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0-M1 through 9.0.97.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

The mitigation for CVE-2024-50379 was incomplete.

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)

Tomcat 11.0.3, 10.1.35 and 9.0.99 onwards will include checks that sun.io.useCanonCaches is set appropriately before allowing the default servlet to be write enabled on a case insensitive file system. Tomcat will also set sun.io.useCanonCaches to false by default where it can.

CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.98](#)
- ...

CVE-2025-24813 [suppress](#)

CISA Known Exploited Vulnerability:

- Product: Apache Tomcat
- Name: Apache Tomcat Path Equivalence Vulnerability
- Date Added: 2025-04-01
- Description: Apache Tomcat contains a path equivalence vulnerability that allows a remote attacker to execute code, disclose information, or inject malicious content via a partial PUT request.
- Required Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
- Due Date: 2025-04-22
- Notes: This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: <https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkq> ; <https://nvd.nist.gov/vuln/detail/CVE-2025-24813>

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0-M1 through 9.0.98.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that was 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 were true, a malicious user was able to perform remote code execution:

- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- application was using Tomcat's file based session persistence with the default storage location
- application included a library that may be leveraged in a deserialization attack

Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

CWE-44 Path Equivalence: 'file.name' (Internal Dot), CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- 134c704f-9b21-4f2e-91b3-4a467353bcc0 - [EXPLOIT](#)
- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE TRACKING](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions up to \(excluding\) 9.0.99](#)
- ...

CVE-2025-31651 [suppress](#)

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. For a subset of unlikely rewrite rule configurations, it was possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.5, from 10.1.0-M1 through 10.1.39, from 9.0.0-M1 through 9.0.102. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.

CWE-116 Improper Encoding or Escaping of Output

CVSSv3:

- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.104](#)
- ...

[CVE-2025-49124](#) suppress

Untrusted Search Path vulnerability in Apache Tomcat installer for Windows. During installation, the Tomcat installer for Windows used icacls.exe without specifying a full path.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0 through 10.1.41, from 9.0.23 through 9.0.105.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100 and 7.0.95 through 7.0.109.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-426 Untrusted Search Path

CVSSv3:

- Base Score: HIGH (8.4)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:2.5/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.23: versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2020-8022](#) suppress

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CWE-276 Incorrect Default Permissions

CVSSv3:

- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.8/RC:R/MAV:A

CVSSv2:

- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

References:

- af854a3a-2127-422b-91ae-364da2661108 - [EXPLOIT,ISSUE TRACKING,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,VENDOR ADVISORY](#)
- meissner@suse.de - [EXPLOIT,ISSUE TRACKING,VENDOR ADVISORY](#)
- meissner@suse.de - [MAILING_LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions up to \(excluding\) 9.0.35-3.57.3](#)
- ...

[CVE-2020-11996](#) suppress

A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.

NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST, VENDOR ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.0; versions up to \(including\) 9.0.35](#)
 - ...

CVE-2020-13934 suppress

An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.

CWE-401 Missing Release of Memory after Effective Lifetime, CWE-476 NULL Pointer Dereference

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
 - Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,RELEASE NOTES,VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING_LIST,RELEASE NOTES,VENDOR ADVISORY](#)
 - security@apache.org - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING_LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.1](#) versions from (including) 9.0.1; versions up to (including) 9.0.36
 - ...

CVE-2020-13935 suppress

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

CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2

- Base Score: MEDIUM (5.0)
 - Vector: /AV:N/AC:L/Au:/N/C:N/I:N/A:P

B-6

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.RELEASE_NOTES.VENDOR ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [NOT_APPLICABLE.THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH.THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISEDY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISEDY](#)

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST RELEASE NOTES VENDOR ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [NOT_APPLICABLE THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.1: versions up to \(including\) 9.0.36](#)
- ...

[CVE-2020-17527](#) suppress

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

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.1: versions up to \(including\) 9.0.35](#)
- ...

[CVE-2021-25122](#) suppress

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0-M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)

- security@apache.org - [PATCH, THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0: versions up to \(including\) 9.0.41](#)
- ...

[CVE-2021-41079](#) suppress

Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

CWE-20 Improper Input Validation, CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST, THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST, VENDOR ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.44](#)
- ...

[CVE-2022-29885](#) suppress

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

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, MITIGATION, VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH, THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST, MITIGATION, VENDOR ADVISORY](#)
- security@apache.org - [MAILING LIST, THIRD PARTY ADVISORY](#)
- security@apache.org - [PATCH, THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.13: versions up to \(including\) 9.0.62](#)
- ...

[CVE-2022-42252](#) suppress

If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, VENDOR ADVISORY](#)
- security@apache.org - [MAILING LIST, VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.68](#)
- ...

[CVE-2023-44487](#) suppress

CISA Known Exploited Vulnerability:

- Product: IETF HTTP/2

- Name: HTTP/2 Rapid Reset Attack Vulnerability
 - Date Added: 2023-10-10
 - Description: HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).
 - Required Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
 - Due Date: 2023-10-31
 - Notes: This vulnerability affects a common open-source component, third-party library, or protocol used by different products. For more information, please see: [HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487 | CISA](https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487): <https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487>; <https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/>; <https://nvd.nist.gov/vuln/detail/CVE-2023-44487>

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

CWE-400 Uncontrolled Resource Consumption, NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.5)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.90](#)
- ...

[CVE-2024-38286](#) suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.35 through 8.5.100 and 7.0.92 through 7.0.109.

Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue.

Apache Tomcat, under certain configurations on any platform, allows an attacker to cause an OutOfMemoryError by abusing the TLS handshake process.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.13: versions up to \(excluding\) 9.0.90](#)
- ...

[CVE-2025-48988](#) suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0-M1 through 9.0.105. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)[THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST](#)[VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2025-48989](#) suppress

Improper Resource Shutdown or Release vulnerability in Apache Tomcat made Tomcat vulnerable to the made you reset attack.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.9, from 10.1.0-M1 through 10.1.43 and from 9.0.0-M1 through 9.0.107. Older, EOL versions may also be affected.

Users are recommended to upgrade to one of versions 11.0.10, 10.1.44 or 9.0.108 which fix the issue.

CWE-404 Improper Resource Shutdown or Release

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [MAILING LIST](#)[VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.108](#)
- ...

[CVE-2025-49125](#) suppress

Authentication Bypass Using an Alternate Path or Channel vulnerability in Apache Tomcat. When using PreResources or PostResources mounted other than at the root of the web application, it was possible to access those resources via an unexpected path. That path was likely not to be protected by the same security constraints as the expected path, allowing those security constraints to be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-288 Authentication Bypass Using an Alternate Path or Channel

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.106](#)
- ...

[CVE-2025-52434](#) suppress

Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Tomcat when using the APR/Native connector. This was particularly noticeable with client initiated closes of HTTP/2 connections.

This issue affects Apache Tomcat: from 9.0.0.M1 through 9.0.106.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 9.0.107, which fixes the issue.

CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [ISSUE TRACKING MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions:

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.107](#)

[CVE-2025-52520](#) suppress

For some unlikely configurations of multipart upload, an Integer Overflow vulnerability in Apache Tomcat could lead to a DoS via bypassing of size limits.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.

CWE-190 Integer Overflow or Wraparound

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - [ISSUE TRACKING MAILING LIST VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*\.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.107](#)
- ...

[CVE-2025-53506](#) suppress

Uncontrolled Resource Consumption vulnerability in Apache Tomcat if an HTTP/2 client did not acknowledge the initial settings frame that reduces the maximum permitted concurrent streams.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106.

The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100.

Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:3.9/RC:R/MAV:A

References:

- security@apache.org - ISSUE TRACKING, MAILING LIST, VENDOR ADVISORY

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:*](#);*;*;*;*;* versions from (including) 9.0.0; versions up to (including) 9.0.106
 - ...

[CVE-2025-46701](#) suppress

Improper Handling of Case Sensitivity vulnerability in Apache Tomcat's GCI servlet allows security constraint bypass of security constraints that apply to the pathInfo component of a URI mapped to the CGI servlet.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.6, from 10.1.0-M1 through 10.1.40, from 9.0.0.M1 through 9.0.104. The following versions were EOL at the time the CVE was created but are

known to be affected: 8.5.0 through 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.7, 10.1.41 or 9.0.105, which fixes the issue.

CWE-178 Improper Handling of Case Sensitivity

CVSSv3:

- Base Score: HIGH (7.3)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST, THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST, VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:**:**:**:**](#) versions from (including) 9.0.0; versions up to (excluding) 9.0.105
 - ...

[CVE-2020-9484](#) suppress

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

CWE-502 Deserialization of Untrusted Data

CVSSv3:

- Base Score: HIGH (7.0)
 - Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.4)
 - Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

References:

- security@apache.org - [THIRD PARTY ADVISORY,VDB ENTRY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.1](#) versions from (including) 9.0.1; versions up to (excluding) 9.0.43
 - ...

[CVE-2021-25329](#) suppress

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

NVD-CWE-noinfo

CVSSv3:

- Base Score: HIGH (7.0)
 - Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:1.0/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.4)
 - Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
 - security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.0:9.0.41](#) versions from (including) 9.0.0; versions up to (including) 9.0.41
 - ...

[CVE-2021-30640](#) suppress

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

CWE-116 Improper Encoding or Escaping of Output

CVSSv3:

- Base Score: MEDIUM (6.5)
 - Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
 - Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.0_46](#): versions from (including) 9.0.0 to (excluding) 9.0.46
 - ...

[CVE-2025-55668](#) suppress

Session Fixation vulnerability in Apache Tomcat via rewrite valve.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWF-384 Session Fixation

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:2.8/RC:R/MAV:A

References:

- security@apache.org - [MAILING_LIST.VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1; versions up to \(excluding\) 9.0.106](#)
- ...

CVE-2024-23672 suppress

Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

CWE-459 Incomplete Cleanup

CVSSv3:

- Base Score: MEDIUM (6.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISED](#)
- security@apache.org - [VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0; versions up to \(excluding\) 9.0.86](#)
- ...

CVE-2022-34305 suppress

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

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C:C:L/I:L/A:N/E:2.8/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.RELEASE NOTES.THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST RELEASE NOTES.THIRD PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST THIRD PARTY ADVISED](#)
- security@apache.org - [THIRD PARTY ADVISED](#)
- security@apache.org - [THIRD PARTY ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.30; versions up to \(including\) 9.0.64](#)
- ...

CVE-2023-41080 suppress

URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92.

Older, EOL versions may also be affected.

The vulnerability is limited to the ROOT (default) web application.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv3:

- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C:C:L/I:L/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [ISSUE TRACKING PATCH.VENDOR ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST.THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISED](#)
- security@apache.org - [ISSUE TRACKING PATCH.VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.0; versions up to \(including\) 9.0.79](#)
- ...

[CVE-2021-24122](#) suppress

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CWE-706 Use of Incorrectly-Resolved Name or Reference, CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVSSv3:

- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(including\) 9.0.1; versions up to \(including\) 9.0.39](#)
- ...

[CVE-2021-33037](#) suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST VENDOR ADVISORY](#)
- security@apache.org - [PATCH THIRD PARTY ADVISORY](#)
- security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:*** versions from \(excluding\) 9.0.0; versions up to \(including\) 9.0.46](#)
- ...

[CVE-2023-42795](#) suppress

Incomplete Cleanup vulnerability in Apache Tomcat. When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next. Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.

CWE-459 Incomplete Cleanup

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.81](#)
- ...

[CVE-2023-45648](#) suppress

Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.

CWE-20 Improper Input Validation, NVD-CWE-Other

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISORY](#)
- security@apache.org - [VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.81](#)
- ...

[CVE-2024-21733](#) suppress

Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43.

Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.

CWE-209 Generation of Error Message Containing Sensitive Information

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,PATCH,THIRD PARTY ADVISORY](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,PATCH,VENDOR ADVISORY](#)
- security@apache.org - [MAILING LIST,PATCH,THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,PATCH,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.1: versions up to \(excluding\) 9.0.44](#)
- ...

[CVE-2024-54677](#) suppress

Uncontrolled Resource Consumption vulnerability in the examples web application provided with Apache Tomcat leads to denial of service.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.1, from 10.1.0-M1 through 10.1.33, from 9.0.0-M1 through 9.9.97. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected.

Users are recommended to upgrade to version 11.0.2, 10.1.34 or 9.0.98, which fixes the issue.

CWE-400 Uncontrolled Resource Consumption

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:3.9/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
- security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***.*.*.*.* versions from \(including\) 9.0.0: versions up to \(excluding\) 9.0.98](#)
- ...

[CVE-2019-17569](#) suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (4.8)
 - Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv2:

- Base Score: MEDIUM (5.8)
 - Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING LIST,VENDOR ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,THIRD PARTY ADVISORY](#)
 - security@apache.org - [MAILING LIST,VENDOR ADVISORY](#)
 - security@apache.org - [PATCH,THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)
 - security@apache.org - [THIRD PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:**:**:**:*](#) versions from (including) 9.0.28; versions up to (including) 9.0.30
 - ...

CVE-2020-1935 suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CVSSv3:

- Base Score: MEDIUM (4.8)
 - Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:2.2/RC:R/MAV:A

CVSSv2.
Base

- Base Score: MEDIUM (3.0)
 - Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

ferences:

 - af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK,MAILING_LIST,THIRD_PARTY ADVISED](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,VENDOR ADVISED](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISORY](#)
 - security@apache.org - [BROKEN_LINK,MAILING_LIST,THIRD_PARTY ADVISED](#)
 - security@apache.org - [MAILING_LIST,THIRD_PARTY ADVISED](#)
 - security@apache.org - [MAILING_LIST,THIRD_PARTY ADVISORY](#)
 - security@apache.org - [MAILING_LIST,VENDOR ADVISED](#)
 - security@apache.org - [THIRD_PARTY ADVISED](#)
 - security@apache.org - [THIRD_PARTY ADVISORY](#)
 - security@apache.org - [THIRD_PARTY ADVISORY](#)
 - security@apache.org - [THIRD_PARTY ADVISED](#)
 - security@apache.org - [THIRD_PARTY ADVISORY](#)
 - security@apache.org - [THIRD_PARTY ADVISORY](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:***](#) versions from (including) 9.0.0; versions up to (including) 9.0.30
 - ...

[CVE-2020-13943](#) suppress

If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

NVD-CWE-noinfo

CVSSv3

- Base Score: MEDIUM (4.3)
 - Vector: CVSS:3.1/AV:N/AC:L/PR:L/U/N/S/L/C:L/I:N/A:N/E:2.8/RC:R/MAV:A

CVSSv2

- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

References:

- af854a3a-2127-422b-91ae-364da2661108 - [BROKEN_LINK](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [PATCH,THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [VENDOR ADVISED](#)
- security@apache.org - [BROKEN_LINK](#)
- security@apache.org - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- security@apache.org - [PATCH,THIRD_PARTY ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)
- security@apache.org - [VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:9.0.30:***:***:*](#)
- ...

[CVE-2023-28708](#) suppress

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

Older, EOL versions may also be affected.

CWE-523 Unprotected Transport of Credentials

CVSSv3:

- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:2.8/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,PATCH,VENDOR ADVISED](#)
- security@apache.org - [MAILING_LIST,PATCH,VENDOR ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(excluding\) 9.0.0: versions up to \(excluding\) 9.0.72](#)
- ...

[CVE-2021-43980](#) suppress

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

CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CVSSv3:

- Base Score: LOW (3.7)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:2.2/RC:R/MAV:A

References:

- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [MAILING_LIST,VENDOR ADVISED](#)
- af854a3a-2127-422b-91ae-364da2661108 - [THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST,THIRD_PARTY ADVISED](#)
- security@apache.org - [MAILING_LIST,VENDOR ADVISED](#)
- security@apache.org - [THIRD_PARTY ADVISED](#)

Vulnerable Software & Versions: ([show all](#))

- [cpe:2.3:a:apache:tomcat:***:***:***:*** versions from \(including\) 9.0.0: versions up to \(including\) 9.0.60](#)
- ...

This report contains data retrieved from the [National Vulnerability Database](#).This report may contain data retrieved from the [CISA Known Exploited Vulnerability Catalog](#).This report may contain data retrieved from the [Github Advisory Database \(via NPM Audit API\)](#).This report may contain data retrieved from [RetireJS](#).This report may contain data retrieved from the [Sonatype OSS Index](#).