DEPENDENCY-CHECK

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:1.0-SNAPSHOT

Scan Information (show less):

- *dependency-check version*: 6.5.3
- *Report Generated On*: Wed, 19 Feb 2025 15:56:24 -0500
- *Dependencies Scanned*: 49 (34 unique)
- *Vulnerable Dependencies*: 21
- *Vulnerabilities Found*: 158
- *Vulnerabilities Suppressed*: 0
- *CurrentEngineRelease*: 12.1.0
- *NVD CVE Checked*: 2025-02-19T14:54:21
- *NVD CVE Modified*: 2025-02-19T14:00:03
- *VersionCheckOn*: 2025-02-19T14:54:21

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evide
accessors-smart-1.2.jar	cpe:2.3:a:json-java_project:json-java:1.2:*:*:*:*:*:*:* cpe:2.3:a:json-smart_project:json-smart:1.2:*:*:*:*:*:*:* cpe:2.3:a:json-smart_project:json-smart-v1:1.2:*:*:*:*:*:*:*	pkg:maven/net.minidev/accessors-smart@1.2	HIGH	4	Low	30
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	2	Highest	33
jackson-core-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:* cpe:2.3:a:json-java_project:json-java:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2	HIGH	2	Low	46
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	40
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	29
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	34
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	43
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	32
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	32
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	8	Highest	27
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	30
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	26
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	12	Highest	29
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	26
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:*:*:*:*:*:*	pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE	CRITICAL	13	Highest	28

	cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*					
spring-hateoas-1.0.3.RELEASE.jar	cpe:2.3:a:vmware:spring_framework:1.0.3:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*:*	pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE	CRITICAL	14	Highest	28
spring-plugin-core-2.0.0.RELEASE.jar	cpe:2.3:a:vmware:spring_framework:2.0.0:release:*:*:*:*:*:*	pkg:maven/org.springframework.plugin/spring-plugin-core@2.0.0.RELEASE	CRITICAL	13	Highest	24
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:springsource: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	HIGH	8	Highest	26
spring-webmvc-5.2.3.RELEASE.jar	cpe:2.3:a:springsource: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	HIGH	2	Highest	28
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	27	Highest	32
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	28	Highest	31

Dependencies

accessors-smart-1.2.jar

Description:

Java reflect give poor performance on getter setter an constructor calls, accessors-smart use ASM to speed up those calls.

License:

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

File Path: /Users/iancoxon/.m2/repository/net/minidev/accessors-smart/1.2/accessors-smart-1.2.jar
MD5: c28b871d258b4d347559d2eb7ecec4a3
SHA1: c592b500269bfde36096641b01238a8350f8aa31
SHA256:0c7c265d62fc007124dc32b91336e9c4272651d629bc5fa1a4e4e3bc758eb2e4
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/net.minidev/accessors-smart@1.2 (*Confidence*:High)
- cpe:2.3:a:json-java_project:json-java:1.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:json-smart_project:json-smart:1.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:json-smart_project:json-smart-v1:1.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

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

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

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

References:
- - [druid-commits] 20210712 [GitHub] [druid] zachjsh merged pull request #11438: Suppress CVE-2021-27568 from json-smart 2.3 dependency
- - [druid-commits] 20210712 [GitHub] [druid] zachjsh opened a new pull request #11438: Suppress CVE-2021-27568 from json-smart 2.3 dependency
- - [druid-commits] 20210712 [druid] branch master updated: Suppress CVE-2021-27568 from json-smart 2.3 dependency (#11438)
- - https://github.com/netplex/json-smart-v1/issues/7
- - https://github.com/netplex/json-smart-v2/issues/60
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:json-smart_project:json-smart-v1:*:*:*:*:*:*:*:* versions up to (excluding) 1.3.2
- ...

CVE-2022-45688 suppress

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

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:

- - https://github.com/dromara/hutool/issues/2748
- - https://github.com/stleary/JSON-java/issues/708

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (excluding) 20230227
- ...

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

References:

- - https://research.jfrog.com/vulnerabilities/stack-exhaustion-in-json-smart-leads-to-denial-of-service-when-parsing-malformed-json-xray-427633/
- - https://security.netapp.com/advisory/ntap-20240621-0006/

Vulnerable Software & Versions:

- cpe:2.3:a:json-smart_project:json-smart:*:*:*:*:*:*:*:* versions up to (excluding) 2.4.9

CVE-2023-5072 suppress

Denial of Service in JSON-Java versions up to and including 20230618. A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.

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

References:

- - http://www.openwall.com/lists/oss-security/2023/12/13/4
- - https://github.com/stleary/JSON-java/issues/758
- - https://github.com/stleary/JSON-java/issues/771
- - https://security.netapp.com/advisory/ntap-20240621-0007/

Vulnerable Software & Versions:

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (including) 20230618

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: /Users/iancoxon/.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

Evidence

Identifiers

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

Published Vulnerabilities

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.

CVSSv2:

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

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

References:

- - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- - [portals-pluto-dev] 20210714 [jira] [Created] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-791 Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- 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

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
- ...

CVE-2023-1932 (OSSINDEX) 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.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2023-1932 for details

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

CVSSv2:

- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/C:/I:/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

Vulnerable Software & Versions (OSSINDEX):

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

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: /Users/iancoxon/.m2/repository/com/fasterxml/jackson/core/jackson-core/2.10.2/jackson-core-2.10.2.jar
MD5: 5514a46e38331f8c8262ea63bf36483e
SHA1: 73d4322a6bda684f676a2b5fe918361c4e5c7cca
SHA256:4c41f22a48f6ebb28752baeb6d25bf09ba4ff0ad8bfb82650dde448928b9da4f
Referenced In Project/Scope:ssl-server:compile

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
- cpe:2.3:a:json-java_project:json-java:2.10.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2022-45688 suppress

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

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:
- - https://github.com/dromara/hutool/issues/2748
- - https://github.com/stleary/JSON-java/issues/708

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (excluding) 20230227
- ...

CVE-2023-5072 suppress

Denial of Service in JSON-Java versions up to and including 20230618. A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.

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

References:
- - http://www.openwall.com/lists/oss-security/2023/12/13/4
- - https://github.com/stleary/JSON-java/issues/758
- - https://github.com/stleary/JSON-java/issues/771
- - https://security.netapp.com/advisory/ntap-20240621-0007/

Vulnerable Software & Versions:

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (including) 20230618

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: /Users/iancoxon/.m2/repository/com/fasterxml/jackson/core/jackson-databind/2.10.2/jackson-databind-2.10.2.jar
MD5: 057751b4e2dd1104be8caad6e9a3e589
SHA1: 0528de95f198afafbcfb0c09d2e43b6e0ea663ec
SHA256:42c25644e35fadfbded1b7f35a8d1e70a86737f190e43aa2c56cea4b96cbda88
Referenced In Project/Scope:ssl-server:compile

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 ('XXE')

CVSSv2:

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

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

References:

- - FEDORA-2021-1d8254899c
- - [druid-commits] 20201208 [GitHub] [druid] jihoonson opened a new pull request #10655: Bump up jackson-databind to 2.10.5.1
- - [flink-issues] 20210121 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- - [flink-issues] 20210122 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- - [hive-dev] 20210223 [jira] [Created] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Assigned] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210315 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210316 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210503 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210510 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210514 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20211012 [jira] [Resolved] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20211012 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [iotdb-commits] 20210325 [iotdb] branch master updated: [IOTDB-1256] upgrade Jackson to 2.11.0 because of loopholes CVE-2020-25649 (#2896)
- - [iotdb-notifications] 20210324 [jira] [Created] (IOTDB-1256) Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 closed pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 opened a new pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210325 [GitHub] [iotdb] jixuan1989 merged pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [kafka-dev] 20201215 Re: [VOTE] 2.7.0 RC5
- - [kafka-dev] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- - [kafka-dev] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-dev] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-jira] 20201205 [GitHub] [kafka] sirocchj opened a new pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] ijuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma merged pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-users] 20201215 Re: [VOTE] 2.7.0 RC5
- - [kafka-users] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- - [kafka-users] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-users] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre commented on pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre merged pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [GitHub] [karaf] svogt opened a new pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [karaf] branch master updated: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [knox-dev] 20210601 [jira] [Created] (KNOX-2614) Upgrade Jackson due to CVE-2020-25649
- - [knox-dev] 20210601 [jira] [Updated] (KNOX-2614) Upgrade jackson-databind to 2.10.5 due to CVE-2020-25649
- - [spark-user] 20210621 Re: CVEs
- - [tomee-commits] 20210127 [jira] [Created] (TOMEE-2965) CVE-2020-25649 - Update jackson databind
- - [turbine-commits] 20210316 svn commit: r1887732 - in /turbine/fulcrum/trunk/json: ./ jackson/ jackson/src/test/org/apache/fulcrum/json/jackson/ jackson2/ jackson2/src/test/org/apache/fulcrum/json/jackson/ jackson2/src/test/org/apache/fulcrum/json/jackson/mixins/
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5.9 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch master updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-dev] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210105 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210106 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210106 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210116 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] asfgit closed pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] edwin092 opened a new pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] nkalmar commented on pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - https://bugzilla.redhat.com/show_bug.cgi?id=1887664
- - https://github.com/FasterXML/jackson-databind/issues/2589
- - https://lists.apache.org/thread.html/r31f4ee7d561d56a0c2c2c6eb1d6ce3e05917ff9654fdbfec05dc2b83%40%3Ccommits.servicecomb.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210108-0007/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html

- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- 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:*:*:*:*:*:*:*:* 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

CVSSv2:

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

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:

- - DSA-5283
- - [debian-lts-announce] 20220502 [SECURITY] [DLA 2990-1] jackson-databind security update
- - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- - https://github.com/FasterXML/jackson-databind/issues/2816
- - https://security.netapp.com/advisory/ntap-20220506-0004/
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- 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

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/UI:N/S:U/C:N/I:N/A:H

References:

- - https://github.com/FasterXML/jackson-databind/issues/3328
- - https://groups.google.com/g/jackson-user/c/OsBsirPM_Vw
- OSSINDEX - [CVE-2021-46877] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3328

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 suppress

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/UI:N/S:U/C:N/I:N/A:H

References:

- - DSA-5283
- - GLSA-202210-21
- - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020
- - https://github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103fef3187f70543d67ca33
- - https://github.com/FasterXML/jackson-databind/issues/3590
- - https://security.netapp.com/advisory/ntap-20221124-0004/
- 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
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3590

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

References:
- - DSA-5283
- - GLSA-202210-21
- - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490
- - https://github.com/FasterXML/jackson-databind/commit/063183589218fec19a9293ed2f17ec53ea80ba88
- - https://github.com/FasterXML/jackson-databind/issues/3582
- - https://security.netapp.com/advisory/ntap-20221118-0008/
- 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

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

References:
- - https://github.com/FasterXML/jackson-databind/issues/3972

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: /Users/iancoxon/.m2/repository/com/jayway/jsonpath/json-path/2.4.0/json-path-2.4.0.jar
MD5: 29169b4b1115bc851e5734ef35ecd42a
SHA1: 765a4401ceb2dc8d40553c2075eb80a8fa35c2ae
SHA256:60441c74fb64e5a480070f86a604941927aaf684e2b513d780fb7a38fb4c5639
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

CVSSv2:

- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/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: /Users/iancoxon/.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

Evidence

Identifiers

- pkg:maven/net.minidev/json-smart@2.3 (*Confidence*:High)
- cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:json-smart_project:json-smart-v2:2.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

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

CVSSv2:

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

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

References:

- - [druid-commits] 20210712 [GitHub] [druid] zachjsh merged pull request #11438: Suppress CVE-2021-27568 from json-smart 2.3 dependency
- - [druid-commits] 20210712 [GitHub] [druid] zachjsh opened a new pull request #11438: Suppress CVE-2021-27568 from json-smart 2.3 dependency
- - [druid-commits] 20210712 [druid] branch master updated: Suppress CVE-2021-27568 from json-smart 2.3 dependency (#11438)
- - https://github.com/netplex/json-smart-v1/issues/7
- - https://github.com/netplex/json-smart-v2/issues/60
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- 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

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:/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

References:
- - https://research.jfrog.com/vulnerabilities/stack-exhaustion-in-json-smart-leads-to-denial-of-service-when-parsing-malformed-json-xray-427633/
- - https://security.netapp.com/advisory/ntap-20240621-0006/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:json-smart_project:json-smart:*:*:*:*:*:*:*:* versions up to (excluding) 2.4.9

log4j-api-2.12.1.jar

Description:

The Apache Log4j API

License:

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

File Path: /Users/iancoxon/.m2/repository/org/apache/logging/log4j/log4j-api/2.12.1/log4j-api-2.12.1.jar
MD5: 4a6f276d4fb426c8d489343c0325bb75
SHA1: a55e6d987f50a515c9260b0451b4fa217dc539cb
SHA256:429534d03bdb728879ab551d469e26f6f7ff4c8a8627f59ac68ab6ef26063515
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1 (*Confidence*:High)
- cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-9488 suppress

Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1

CWE-295 Improper Certificate Validation

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

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

References:
- - DSA-5020
- - [db-torque-dev] 20200715 Build failed in Jenkins: Torque4-trunk #685
- - [db-torque-dev] 20210127 Re: Items for our (delayed) quarterly report to the board?
- - [db-torque-dev] 20210128 Antwort: Re: Items for our (delayed) quarterly report to the board?
- - [debian-lts-announce] 20211226 [SECURITY] [DLA 2852-1] apache-log4j2 security update
- - [flink-issues] 20210510 [GitHub] [flink] zentol opened a new pull request #15879: [FLINK-22407][build] Bump log4j to 2.24.1
- - [hive-dev] 20201207 [jira] [Created] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-dev] 20210216 [jira] [Created] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Assigned] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Work started] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201208 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201208 [jira] [Work logged] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20210125 [jira] [Work logged] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20210209 [jira] [Resolved] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20210216 [jira] [Assigned] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20210216 [jira] [Resolved] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20210218 [jira] [Updated] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [kafka-dev] 20200514 [jira] [Created] (KAFKA-9996) upgrade zookeeper to 3.5.8 to address security vulnerabilities
- - [kafka-dev] 20200514 [jira] [Created] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488
- - [kafka-jira] 20200514 [jira] [Created] (KAFKA-9996) upgrade zookeeper to 3.5.8 to address security vulnerabilities
- - [kafka-jira] 20200514 [jira] [Created] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488
- - [kafka-jira] 20200515 [jira] [Commented] (KAFKA-9997) upgrade log4j lib to address CVE-2020-9488
- - [kafka-users] 20210617 vulnerabilities
- - [mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar
- - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- - [zookeeper-commits] 20200504 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488
- - [zookeeper-commits] 20200504 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488
- - [zookeeper-commits] 20200504 [zookeeper] branch master updated: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488
- - [zookeeper-dev] 20200504 [jira] [Created] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-dev] 20200504 log4j SmtpAppender related CVE
- - [zookeeper-issues] 20200504 [jira] [Assigned] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-issues] 20200504 [jira] [Commented] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-issues] 20200504 [jira] [Created] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-issues] 20200504 [jira] [Resolved] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-issues] 20200504 [jira] [Updated] (ZOOKEEPER-3817) owasp failing due to CVE-2020-9488
- - [zookeeper-notifications] 20200504 Build failed in Jenkins: zookeeper-master-maven-owasp #489
- - [zookeeper-notifications] 20200504 [GitHub] [zookeeper] symat commented on pull request #1346: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488
- - [zookeeper-notifications] 20200504 [GitHub] [zookeeper] symat opened a new pull request #1346: ZOOKEEPER-3817: suppress log4j SmtpAppender related CVE-2020-9488
- - https://issues.apache.org/jira/browse/LOG4J2-2819
- - https://lists.apache.org/thread.html/rbc7642b9800249553f13457e46b813bea1aec99d2bc9106510e00ff3%40%3Ctorque-dev.db.apache.org%3E
- - https://lists.apache.org/thread.html/re024d86dffa72ad800f2848d0c77ed93f0b78ee808350b477a6ed987%40%3Cgitbox.hive.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200504-0003/
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* versions from (including) 2.4; versions up to (excluding) 2.12.3
- ...

logback-classic-1.2.3.jar

Description:

logback-classic module

License:

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

File Path: /Users/iancoxon/.m2/repository/ch/qos/logback/logback-classic/1.2.3/logback-classic-1.2.3.jar

MD5: 64f7a68f931aed8e5ad8243470440f0b
SHA1: 7c4f3c474fb2c041d8028740440937705ebb473a
SHA256:fb53f8539e7fcb8f093a56e138112056ec1dc809ebb020b59d8a36a5ebac37e0
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

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

CVSSv2:

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

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

References:

- - 20220721 Open-Xchange Security Advisory 2022-07-21
- - http://logback.qos.ch/news.html
- - http://packetstormsecurity.com/files/167794/Open-Xchange-App-Suite-7.10.x-Cross-Site-Scripting-Command-Injection.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-371761.pdf
- - https://github.com/cn-panda/logbackRceDemo
- - https://jira.qos.ch/browse/LOGBACK-1591
- - https://security.netapp.com/advisory/ntap-20211229-0001/
- OSSINDEX - [CVE-2021-42550] CWE-502: Deserialization of Untrusted Data
- OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591

Vulnerable Software & Versions: (show all)

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

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

References:

- - https://logback.qos.ch/news.html#1.3.12
- - https://security.netapp.com/advisory/ntap-20241129-0012/
- 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

Vulnerable Software & Versions: (show all)

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

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/lgpl-2.1.html

File Path: /Users/iancoxon/.m2/repository/ch/qos/logback/logback-core/1.2.3/logback-core-1.2.3.jar
MD5: 841fc80c6edff60d947a3872a2db4d45
SHA1: 864344400c3d4d92dfeb0a305dc87d953677c03c
SHA256:5946d837fe6f960c02a53eda7a6926ecc3c758bbdd69aa453ee429f858217f22
Referenced In Project/Scope:ssl-server:compile

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-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

CVSSv2:
- Base Score: HIGH (8.5)
- Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

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

References:
- - 20220721 Open-Xchange Security Advisory 2022-07-21
- - http://logback.qos.ch/news.html
- - http://packetstormsecurity.com/files/167794/Open-Xchange-App-Suite-7.10.x-Cross-Site-Scripting-Command-Injection.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-371761.pdf
- - https://github.com/cn-panda/logbackRceDemo
- - https://jira.qos.ch/browse/LOGBACK-1591
- - https://security.netapp.com/advisory/ntap-20211229-0001/
- OSSINDEX - [CVE-2021-42550] CWE-502: Deserialization of Untrusted Data
- OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591

Vulnerable Software & Versions: (show all)

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

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

References:
- - https://logback.qos.ch/news.html#1.3.12
- - https://security.netapp.com/advisory/ntap-20241129-0012/
- 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

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-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 (5.9)
- Vector: /AV:L/AC:L/Au:/C:/I:/A:

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-jwxv

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 (2.4)
- Vector: /AV:L/AC:L/Au:/C:/I:/A:

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-gvf4

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: /Users/iancoxon/.m2/repository/org/yaml/snakeyaml/1.25/snakeyaml-1.25.jar
MD5: 6f7d5b8f596047aae07a3bf6f23a0bf2
SHA1: 8b6e01ef661d8378ae6dd7b511a7f2a33fae1421
SHA256:b50ef33187e7dc922b26dbe4dd0fdb3a9cf349e75a08b95269901548eee546eb
Referenced In Project/Scope:ssl-server:runtime

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-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')

CVSSv2:

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

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:

- - FEDORA-2020-23012fafbc
- - FEDORA-2020-599514b47e
- - GLSA-202305-28
- - [atlas-commits] 20200915 [atlas] branch master updated: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)
- - [atlas-commits] 20200916 [atlas] 02/02: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab closed pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #110: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [GitHub] [atlas] nixonrodrigues commented on pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [jira] [Created] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [jira] [Updated] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200915 [GitHub] [atlas] nixonrodrigues merged pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200915 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200916 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [cassandra-commits] 20200930 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Created] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201001 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201002 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201002 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201007 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201007 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [cassandra] branch trunk updated: Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-pr] 20200907 [GitHub] [cassandra] crazylab opened a new pull request #736: Upgrade to a snakeyaml version without CVE
- - [hadoop-common-commits] 20201028 [hadoop] branch branch-3.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20201028 [hadoop] branch trunk updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20211008 [hadoop] branch branch-3.2 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20211008 [hadoop] branch branch-3.2.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-dev] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200830 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200831 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200909 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201026 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201027 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201028 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201028 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211006 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211008 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211008 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [kafka-users] 20210617 vulnerabilities
- - [phoenix-dev] 20210419 [GitHub] [phoenix-omid] richardantal opened a new pull request #93: OMID-207 Upgrade to snakeyaml 1.26 due to CVE-2017-18640
- - [phoenix-dev] 20210419 [jira] [Created] (OMID-207) Upgrade to snakeyaml 1.26 due to CVE-2017-18640
- - [pulsar-commits] 20200830 [GitHub] [pulsar] codelipenghui commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy edited a comment on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200907 [GitHub] [pulsar] jiazhai closed issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion
- - https://bitbucket.org/asomov/snakeyaml/wiki/Billion%20laughs%20attack
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/377
- - https://bitbucket.org/snakeyaml/snakeyaml/wiki/Changes
- - https://lists.apache.org/thread.html/r4c682fb8cf69dd14162439656a6ebdf42ea6ad0e4edba95907ea3f14%40%3Ccommits.servicecomb.apache.org%3E
- - https://lists.apache.org/thread.html/r900e020760c89f082df1c6e0d46320eba721e4e47bb9eb521e68cd95%40%3Ccommits.servicecomb.apache.org%3E
- - https://mvnrepository.com/artifact/org.yaml/snakeyaml/1.25/usages
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- 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

Vulnerable Software & Versions: (show all)

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

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 SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

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

References:
- - http://packetstormsecurity.com/files/175095/PyTorch-Model-Server-Registration-Deserialization-Remote-Code-Execution.html
- - http://www.openwall.com/lists/oss-security/2023/11/19/1
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/561/cve-2022-1471-vulnerability-in#comment-64581479
- - https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2
- - https://github.com/mbechler/marshalsec
- - https://groups.google.com/g/kubernetes-security-announce/c/mwrakFaEdnc
- - https://security.netapp.com/advisory/ntap-20230818-0015/
- - https://security.netapp.com/advisory/ntap-20240621-0006/
- - https://www.github.com/mbechler/marshalsec/blob/master/marshalsec.pdf?raw=true
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 2.0

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

References:
- - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- - https://bitbucket.org/snakeyaml/snakeyaml/commits/fc300780da21f4bb92c148bc90257201220cf174
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/525
- - https://github.com/snakeyaml/snakeyaml/commit/fc300780da21f4bb92c148bc90257201220cf174
- - https://security.netapp.com/advisory/ntap-20240315-0010/
- - https://security.snyk.io/vuln/SNYK-JAVA-ORGYAML-2806360
- 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

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

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

References:
- - GLSA-202305-28
- - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/525/got-stackoverflowerror-for-many-open
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47024
- - https://security.netapp.com/advisory/ntap-20240315-0010/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 1.31

CVE-2022-38750 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

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

References:

- - GLSA-202305-28
- - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027
- - https://security.netapp.com/advisory/ntap-20240315-0010/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 1.31

CVE-2022-38751 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

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

References:

- - GLSA-202305-28
- - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039
- - https://security.netapp.com/advisory/ntap-20240315-0010/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 1.31

CVE-2022-38752 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 stack-overflow.

CWE-787 Out-of-bounds Write

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

References:

- - GLSA-202305-28
- - https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverflow-oss-fuzz-47081
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081
- - https://security.netapp.com/advisory/ntap-20240315-0009/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 1.32

CVE-2022-41854 suppress

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

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

References:

- - FEDORA-2022-8a4e8aa190
- - FEDORA-2022-c01dd659fa
- - FEDORA-2023-27ec59a486
- - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355
- - https://security.netapp.com/advisory/ntap-20240315-0009/
- - https://security.netapp.com/advisory/ntap-20240621-0006/
- 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

Vulnerable Software & Versions:

- cpe:2.3:a:snakeyaml_project:snakeyaml:*:*:*:*:*:*:*:* versions up to (excluding) 1.32

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: /Users/iancoxon/.m2/repository/org/springframework/boot/spring-boot/2.2.4.RELEASE/spring-boot-2.2.4.RELEASE.jar
MD5: 24de0cfd8ea74b903b562b43cbc5eb13
SHA1: 225a4fd31156c254e3bb92adb42ee8c6de812714
SHA256:176befc7b90e8498f44e21994a70d69ba360ef1e858ff3cea8282e802372daf2
Referenced In Project/Scope:ssl-server:compile

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-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

CVSSv2:

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

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

References:

- - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- 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/JLLeitschuh/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

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_boot:*:*:*:*:*:*:*:* versions up to (excluding) 2.2.11

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

References:

- - https://security.netapp.com/advisory/ntap-20230601-0009/
- - https://spring.io/blog/2023/05/18/spring-boot-2-5-15-and-2-6-15-available-now
- - https://spring.io/security/cve-2023-20873

Vulnerable Software & Versions: (show all)

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

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 ('Resource Exhaustion')

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:
- - https://security.netapp.com/advisory/ntap-20230703-0008/
- - https://spring.io/security/cve-2023-20883

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: /Users/iancoxon/.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: ec75d01d212b5229c16d872fb127744c0ed46ed8
SHA256:eb4d4ad19fe1724fd02cfce9c467c0b67766b5a4a54d0e54fc51826d9e3d87b8
Referenced In Project/Scope:ssl-server:compile

Evidence

Related Dependencies

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-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

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

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

References:
- - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_boot:*:*:*:*:*:*:*:* versions up to (excluding) 2.2.11

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

References:

- - https://security.netapp.com/advisory/ntap-20230601-0009/
- - https://spring.io/blog/2023/05/18/spring-boot-2-5-15-and-2-6-15-available-now
- - https://spring.io/security/cve-2023-20873

Vulnerable Software & Versions: (show all)

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

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 ('Resource Exhaustion')

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:

- - https://security.netapp.com/advisory/ntap-20230703-0008/
- - https://spring.io/security/cve-2023-20883

Vulnerable Software & Versions: (show all)

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

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: /Users/iancoxon/.m2/repository/org/springframework/spring-core/5.2.3.RELEASE/spring-core-5.2.3.RELEASE.jar
MD5: ae11e44d9eff630186b9e095e70b59de
SHA1: 3734223040040e8c3fecd5faa3ae8a1ed6da146b
SHA256:6df908f4deaeefd2b03b56a00246cc0dc0d941d9636e811025bc6fc5a2a44851
Referenced In Project/Scope:ssl-server:compile

Evidence

Related Dependencies

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-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

CVSSv2:

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

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

References:

- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 6.0.0

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

CVSSv2:

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

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

References:

- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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

CVSSv2:

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

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

References:

- - https://tanzu.vmware.com/security/cve-2021-22060
- - https://www.oracle.com/security-alerts/cpuapr2022.html

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.

NVD-CWE-Other

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20211125-0005/
- - https://tanzu.vmware.com/security/cve-2021-22096
- - https://www.oracle.com/security-alerts/cpuapr2022.html

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-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-668 Exposure of Resource to Wrong Sphere

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20210713-0005/
- - https://tanzu.vmware.com/security/cve-2021-22118
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-2022-22950 suppress

n 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

CVSSv2:

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

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

References:

- - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22965 suppress

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')

CVSSv2:

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

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

References:

- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968
- - https://www.oracle.com/security-alerts/cpujul2022.html

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220616-0003/
- - https://tanzu.vmware.com/security/cve-2022-22971
- - https://www.oracle.com/security-alerts/cpujul2022.html

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.

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

References:

- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

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-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

References:

- - https://security.netapp.com/advisory/ntap-20240524-0015/
- - https://spring.io/security/cve-2023-20863

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
- ...

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

Description:

Spring Data REST - WebMVC

File Path: /Users/iancoxon/.m2/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
SHA256:7694c509ffaff229d45630d2ee68525588f80d2740deeef7642696f1440043d1
Referenced In Project/Scope:ssl-server:compile

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 URIs that can potentially be exposed for unauthorized access depending on the Spring Security configuration.

CWE-200 Information Exposure

CVSSv2:

- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/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

CVSSv2:

- Base Score: LOW (3.7)
- Vector: /AV:N/AC:H/Au:/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: /Users/iancoxon/.m2/repository/org/springframework/spring-expression/5.2.3.RELEASE/spring-expression-5.2.3.RELEASE.jar
MD5: f2d2fe0e4f9b9b23b03d07839393de5a
SHA1: d0c6bb10758805b2153c589686b8045554bfac2d
SHA256:1ba798e1f4da9e5ad68e67d7e7abe39f141674762c8755d952edeb0380d384b9
Referenced In Project/Scope:ssl-server:compile

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-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

CVSSv2:

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

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

References:

- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 6.0.0

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

CVSSv2:

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

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

References:

- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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

CVSSv2:

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

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

References:

- - https://tanzu.vmware.com/security/cve-2021-22060
- - https://www.oracle.com/security-alerts/cpuapr2022.html

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.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

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

References:
- - https://security.netapp.com/advisory/ntap-20211125-0005/
- - https://tanzu.vmware.com/security/cve-2021-22096
- - https://www.oracle.com/security-alerts/cpuapr2022.html

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-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-668 Exposure of Resource to Wrong Sphere

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

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

References:
- - https://security.netapp.com/advisory/ntap-20210713-0005/
- - https://tanzu.vmware.com/security/cve-2021-22118
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-2022-22950 suppress

n 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

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

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

References:
- - https://tanzu.vmware.com/security/cve-2022-22950
- 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

Vulnerable Software & Versions: (show all)

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

CVE-2022-22965 suppress

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')

CVSSv2:
- Base Score: HIGH (7.5)

- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

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

References:

- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968
- - https://www.oracle.com/security-alerts/cpujul2022.html

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220616-0003/
- - https://tanzu.vmware.com/security/cve-2022-22971
- - https://www.oracle.com/security-alerts/cpujul2022.html

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.

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

References:
- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861
- OSSINDEX - [CVE-2023-20861] CWE-noinfo
- 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

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-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

References:
- - https://security.netapp.com/advisory/ntap-20240524-0015/
- - https://spring.io/security/cve-2023-20863
- 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

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 (5.3)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

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:*:*:*:*:*:*:*

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: /Users/iancoxon/.m2/repository/org/springframework/hateoas/spring-hateoas/1.0.3.RELEASE/spring-hateoas-1.0.3.RELEASE.jar
MD5: efbda177ffbc4a8c7a693080528c9cd8
SHA1: 35c3514a8336d31f346f7b5c99de2f1ee32611ac
SHA256:5a54edfd6ae2e6a85bd694682a358a0a55282f426623da59d47d879de3e1846d
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2013-4152 suppress

The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disable entity resolution, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via an XML external entity declaration in conjunction with an entity reference in a (1) DOMSource, (2) StAXSource, (3) SAXSource, or (4) StreamSource, aka an XML External Entity (XXE) issue.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- - 20131102 XXE Injection in Spring Framework
- - 56247
- - 57915
- - 61951
- - DSA-2842
- - RHSA-2014:0212
- - RHSA-2014:0245
- - RHSA-2014:0254
- - RHSA-2014:0400
- - http://www.gopivotal.com/security/cve-2013-4152
- - https://github.com/spring-projects/spring-framework/pull/317/files
- - https://jira.springsource.org/browse/SPR-10806

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.3
- ...

CVE-2013-7315 suppress

The Spring MVC in Spring Framework before 3.2.4 and 4.0.0.M1 through 4.0.0.M2 does not disable external entity resolution for the StAX XMLInputFactory, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML with JAXB, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152. NOTE: this issue was SPLIT from CVE-2013-4152 due to different affected versions.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- - 20131102 XXE Injection in Spring Framework
- - 77998
- - DSA-2842
- - http://www.gopivotal.com/security/cve-2013-4152
- - https://jira.springsource.org/browse/SPR-10806

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.3
- ...

CVE-2014-0054 suppress

The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4152, CVE-2013-7315, and CVE-2013-6429.

CWE-352 Cross-Site Request Forgery (CSRF)

CVSSv2:

- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:

- - 57915
- - 66148
- - RHSA-2014:0400
- - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- - https://jira.spring.io/browse/SPR-11376

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.7
- ...

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

CVSSv2:

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

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

References:

- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 6.0.0

CVE-2018-11039 suppress

Spring Framework (versions 5.0.x prior to 5.0.7, versions 4.3.x prior to 4.3.18, and older unsupported versions) allow web applications to change the HTTP request method to any HTTP method (including TRACE) using the HiddenHttpMethodFilter in Spring MVC. If an application has a pre-existing XSS vulnerability, a malicious user (or attacker) can use this filter to escalate to an XST (Cross Site Tracing) attack.

NVD-CWE-noinfo

CVSSv2:

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

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

References:

- - 107984
- - [debian-lts-announce] 20210423 [SECURITY] [DLA 2635-1] libspring-java security update
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-11039
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.18
- ...

CVE-2018-11040 suppress

Spring Framework, versions 5.0.x prior to 5.0.7 and 4.3.x prior to 4.3.18 and older unsupported versions, allows web applications to enable cross-domain requests via JSONP (JSON with Padding) through AbstractJsonpResponseBodyAdvice for REST controllers and MappingJackson2JsonView for browser requests. Both are not enabled by default in Spring Framework nor Spring Boot, however, when MappingJackson2JsonView is configured in an application, JSONP support is automatically ready to use through the "jsonp" and "callback" JSONP parameters, enabling cross-domain requests.

CWE-829 Inclusion of Functionality from Untrusted Control Sphere

CVSSv2:

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

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

References:

- - [debian-lts-announce] 20210423 [SECURITY] [DLA 2635-1] libspring-java security update
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-11040
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.18
- ...

CVE-2018-1257 suppress

Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attack.

NVD-CWE-noinfo

CVSSv2:

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

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

References:

- - 104260
- - RHSA-2018:1809
- - RHSA-2018:3768
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-1257
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.17
- ...

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

CVSSv2:

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

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

References:

- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-

- 5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.29
- ...

CVE-2022-22950 suppress

n 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

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

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

References:
- - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22965 suppress

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')

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

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

References:
- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

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

References:
- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968

- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 5.2.0
- ...

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

CVSSv2:

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

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

References:

- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* 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.

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

References:

- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

Vulnerable Software & Versions: (show all)

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

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-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

References:

- - https://spring.io/security/cve-2023-34036
- 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

Vulnerable Software & Versions: (show all)

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

spring-plugin-core-2.0.0.RELEASE.jar

Description:

Core plugin infrastructure

File Path: /Users/iancoxon/.m2/repository/org/springframework/plugin/spring-plugin-core/2.0.0.RELEASE/spring-plugin-core-2.0.0.RELEASE.jar
MD5: a89cd7b77db3ed7d0c9ea71ee9784e2e
SHA1: 95fc8c13037630f4aba9c51141f535becec00fe6
SHA256:6e6d026d6b572495533692173a264c6959f48d5ef7f3d6faf4555a577d4a38d2
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/org.springframework.plugin/spring-plugin-core@2.0.0.RELEASE (*Confidence*:High)
- cpe:2.3:a:vmware:spring_framework:2.0.0:release:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2013-4152 suppress

The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disable entity resolution, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via an XML external entity declaration in conjunction with an entity reference in a (1) DOMSource, (2) StAXSource, (3) SAXSource, or (4) StreamSource, aka an XML External Entity (XXE) issue.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- - 20131102 XXE Injection in Spring Framework
- - 56247
- - 57915
- - 61951
- - DSA-2842
- - RHSA-2014:0212
- - RHSA-2014:0245
- - RHSA-2014:0254
- - RHSA-2014:0400
- - http://www.gopivotal.com/security/cve-2013-4152
- - https://github.com/spring-projects/spring-framework/pull/317/files
- - https://jira.springsource.org/browse/SPR-10806

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.3
- ...

CVE-2013-7315 suppress

The Spring MVC in Spring Framework before 3.2.4 and 4.0.0.M1 through 4.0.0.M2 does not disable external entity resolution for the StAX XMLInputFactory, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML with JAXB, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152. NOTE: this issue was SPLIT from CVE-2013-4152 due to different affected versions.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- - 20130822 CVE-2013-4152 XML External Entity (XXE) injection in Spring Framework
- - 20131102 XXE Injection in Spring Framework
- - 77998
- - DSA-2842
- - http://www.gopivotal.com/security/cve-2013-4152
- - https://jira.springsource.org/browse/SPR-10806

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.3
- ...

CVE-2014-0054 suppress

The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4152, CVE-2013-7315, and CVE-2013-6429.

CWE-352 Cross-Site Request Forgery (CSRF)

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- - 57915
- - 66148
- - RHSA-2014:0400
- - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- - https://jira.spring.io/browse/SPR-11376

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 3.2.7
- ...

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

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

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

References:
- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions:

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 6.0.0

CVE-2018-11039 suppress

Spring Framework (versions 5.0.x prior to 5.0.7, versions 4.3.x prior to 4.3.18, and older unsupported versions) allow web applications to change the HTTP request method to any HTTP method (including TRACE) using the HiddenHttpMethodFilter in Spring MVC. If an application has a pre-existing XSS vulnerability, a malicious user (or attacker) can use this filter to escalate to an XST (Cross Site Tracing) attack.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

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

References:
- - 107984
- - [debian-lts-announce] 20210423 [SECURITY] [DLA 2635-1] libspring-java security update
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-11039
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.18
- ...

CVE-2018-11040 suppress

Spring Framework, versions 5.0.x prior to 5.0.7 and 4.3.x prior to 4.3.18 and older unsupported versions, allows web applications to enable cross-domain requests via JSONP (JSON with Padding) through AbstractJsonpResponseBodyAdvice for REST controllers and MappingJackson2JsonView for browser requests. Both are not enabled by default in Spring Framework nor Spring Boot, however, when MappingJackson2JsonView is configured in an application, JSONP support is automatically ready to use through the "jsonp" and "callback" JSONP parameters, enabling cross-domain requests.

CWE-829 Inclusion of Functionality from Untrusted Control Sphere

CVSSv2:

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

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

References:

- - [debian-lts-announce] 20210423 [SECURITY] [DLA 2635-1] libspring-java security update
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-11040
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.18
- ...

CVE-2018-1257 suppress

Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attack.

NVD-CWE-noinfo

CVSSv2:

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

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

References:

- - 104260
- - RHSA-2018:1809
- - RHSA-2018:3768
- - http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
- - https://pivotal.io/security/cve-2018-1257
- - https://www.oracle.com/security-alerts/cpujan2020.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
- - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- - https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.17
- ...

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

CVSSv2:

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

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

References:

- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-

5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 4.3.29
- ...

CVE-2022-22950 suppress

n 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

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

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

References:
- - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22965 suppress

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')

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

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

References:
- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

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

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

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

References:
- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968

- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (excluding) 5.2.0
- ...

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

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:N/A:P

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

References:
- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* 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.

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

References:
- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

Vulnerable Software & Versions: (show all)

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

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: /Users/iancoxon/.m2/repository/org/springframework/spring-web/5.2.3.RELEASE/spring-web-5.2.3.RELEASE.jar
MD5: a89d66690cd14159aa6ac1e875e54411
SHA1: dd386a02e40b915ab400a3bf9f586d2dc4c0852c
SHA256:25d264969c624cb8103a7f2b36b148ea1be8b87780c4758e7f9a6e2bc8416d76
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/org.springframework/spring-web@5.2.3.RELEASE (*Confidence*:High)
- cpe:2.3:a:springsource: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 (OSSINDEX) 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

CVSSv2:

- Base Score: HIGH (9.8)
- Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

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.gypsyengineer.com/en/security/detecting-dangerous-spring-exporters-with-codeql.html
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/24434
- OSSIndex - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2020-5421 (OSSINDEX) 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.

CWE-noinfo

CVSSv2:

- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:H/Au:/C:L/I:H/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

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2021-22096 (OSSINDEX) 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

CVSSv2:

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

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2021-22118 (OSSINDEX) 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.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2021-22118 for details

CWE-269 Improper Privilege Management

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/Au:/C:H/I:H/A:H

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

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')

CVSSv2:

- Base Score: HIGH (8.1)
- Vector: /AV:N/AC:L/Au:/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')

CVSSv2:

- Base Score: HIGH (8.1)
- Vector: /AV:N/AC:L/Au:/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-2024-38809 (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 ('Resource Exhaustion')

CVSSv2:

- Base Score: HIGH (8.7)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

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-2024-38828 (OSSINDEX) suppress

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

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:

- Base Score: MEDIUM (6.9)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

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:*:*:*:*:*:*:*

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: /Users/iancoxon/.m2/repository/org/springframework/spring-webmvc/5.2.3.RELEASE/spring-webmvc-5.2.3.RELEASE.jar
MD5: 867cc7369d453637b5042ee4d6931a78
SHA1: 745a62502023d2496b565b7fe102bb1ee229d6b7
SHA256:b3b0a2477e67b050dd5c08dc96e76db5950cbccba075e782c24f73eda49a0160
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE (*Confidence*:High)
- cpe:2.3:a:springsource: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-2021-22060 (OSSINDEX) 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.

CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:L/Au:/C:N/I:L/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

Vulnerable Software & Versions (OSSINDEX):

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

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:

* the Spring Security HTTP Firewall https://docs.spring.io/spring-security/reference/servlet/exploits/firewall.html is in use
* the application runs on Tomcat or Jetty

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

CVSSv2:
- Base Score: HIGH (8.2)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

References:
- OSSINDEX - [CVE-2024-38816] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38816
- OSSIndex - https://spring.io/security/cve-2024-38816

Vulnerable Software & Versions (OSSINDEX):

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

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: /Users/iancoxon/.m2/repository/org/apache/tomcat/embed/tomcat-embed-core/9.0.30/tomcat-embed-core-9.0.30.jar
MD5: f9e49f66756f133157f19e617af26ffe
SHA1: ad32909314fe2ba02cec036434c0addd19bcc580
SHA256:b1415eecbc9f14e3745c1bfd41512a1b8e1af1332a7beaed4be30b2e0ba7b330
Referenced In Project/Scope:ssl-server:compile

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-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 Smuggling')

CVSSv2:
- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:
- - DSA-4673
- - DSA-4680
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [tomcat-announce] 20200224 [SECURITY] CVE-2019-17569 HTTP Request Smuggling
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - https://security.netapp.com/advisory/ntap-20200327-0005/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345

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-2020-11996 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

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

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:
- - DSA-4727
- - USN-4596-1
- - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release17.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release18.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch trunk updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)

- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200701 [jira] [Reopened] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Comment Edited] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20210301 [jira] [Updated] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-users] 20201008 Is Tomcat7 supports HTTP2
- - https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200709-0002/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:1051
- - openSUSE-SU-2020:1063

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 Improper Release of Memory Before Removing Last Reference ('Memory Leak'), CWE-476 NULL Pointer Dereference

CVSSv2:

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

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:

- - DSA-4727
- - USN-4596-1
- - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- - [tomcat-dev] 20200818 [Bug 64671] HTTP/2 Stream.receivedData method throwing continuous NullPointerException in the logs
- - https://lists.apache.org/thread.html/r61f411cf82488d6ec213063fc15feeeb88e31b0ca9c29652ee4f962e%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200724-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:1102
- - openSUSE-SU-2020:1111

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-2020-13935 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')

CVSSv2:

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

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:

- - DSA-4727
- - USN-4448-1
- - USN-4596-1
- - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- - [tomcat-users] 20201118 Re: Strange crash-on-takeoff, Tomcat 7.0.104
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- - https://lists.apache.org/thread.html/rd48c72bd3255bda87564d4da3791517c074d94f8a701f93b85752651%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200724-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - openSUSE-SU-2020:1102
- - openSUSE-SU-2020:1111

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-2020-13943 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

CVSSv2:

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

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

References:

- - DSA-4835
- - [debian-lts-announce] 20201014 [SECURITY] [DLA 2407-1] tomcat8 security update
- - https://lists.apache.org/thread.html/r4a390027eb27e4550142fac6c8317cc684b157ae314d31514747f307%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20201016-0007/
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - openSUSE-SU-2020:1799
- - openSUSE-SU-2020:1842

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*
- ...

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 Information Exposure

CVSSv2:

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

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

References:

- - DSA-4835
- - GLSA-202012-23
- - [announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [debian-lts-announce] 20201216 [SECURITY] [DLA 2495-1] tomcat8 security update
- - [guacamole-issues] 20201206 [jira] [Commented] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- - [guacamole-issues] 20201206 [jira] [Created] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- - [oss-security] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-dev] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-dev] 20201203 svn commit: r1884073 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210114 svn commit: r1885488 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-users] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-users] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomee-commits] 20201207 [jira] [Assigned] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - [tomee-commits] 20201207 [jira] [Created] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - [tomee-commits] 20210319 [jira] [Updated] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - https://lists.apache.org/thread.html/rce5ac9a40173651d540babce59f6f3825f12c6d4e886ba00823b11e5%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20201210-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html

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-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 Smuggling')

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:

- - DSA-4673
- - DSA-4680
- - USN-4448-1
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1935 HTTP Request Smuggling
- - [tomcat-dev] 20210428 [Bug 65272] Problems proccessing HTTP request without CR in last versions
- - [tomcat-users] 20200724 CVE-2020-1935
- - [tomcat-users] 20200724 RE: CVE-2020-1935
- - [tomcat-users] 20200724 Re: CVE-2020-1935
- - [tomcat-users] 20200726 Re: CVE-2020-1935
- - [tomcat-users] 20200727 RE: CVE-2020-1935
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - https://security.netapp.com/advisory/ntap-20200327-0005/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345

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-2020-1938 suppress

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

CVSSv2:

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

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

References:

- - DSA-4673
- - DSA-4680
- - FEDORA-2020-04ac174fa9
- - FEDORA-2020-0e42878ba7
- - FEDORA-2020-c870aa8378
- - GLSA-202003-43
- - [announce] 20210125 Apache Software Foundation Security Report: 2020
- - [announce] 20210223 Re: Apache Software Foundation Security Report: 2020
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- - [httpd-bugs] 20200319 [Bug 53098] mod_proxy_ajp: patch to set worker secret passed to tomcat
- - [ofbiz-commits] 20200227 [ofbiz-plugins] branch release17.12 updated: Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938) (OFBIZ-11407)
- - [ofbiz-notifications] 20200225 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200225 [jira] [Updated] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200227 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Comment Edited] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-dev] 20200304 Re: Tagging 10.0.x, 9.0.x, 8.5.x
- - [tomcat-dev] 20200309 [Bug 64206] Answer file not being used
- - [tomcat-dev] 20200625 svn commit: r1879208 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20200301 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200302 AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200304 Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Aw: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Re: Aw: Re: Fix for CVE-2020-1938

- - [tomcat-users] 20200309 Re: Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check)
- - [tomcat-users] 20200310 Aw: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200310 Re: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200413 RE: Alternatives for AJP
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2789) TomEE plus is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200320 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Resolved] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-dev] 20200311 CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200311 Re: CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200316 RE: CVE-2020-8840 on TomEE 8.0.1
- - [tomee-users] 20200723 Re: TomEE on Docker
- - http://support.blackberry.com/kb/articleDetail?articleNumber=000062739
- - https://security.netapp.com/advisory/ntap-20200226-0002/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345
- - openSUSE-SU-2020:0597

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-2020-9484 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

CVSSv2:

- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

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

References:

- - 20200602 [CVE-2020-9484] Apache Tomcat RCE via PersistentManager
- - DSA-4727
- - FEDORA-2020-ce396e7d5c
- - FEDORA-2020-d9169235a8
- - GLSA-202006-21
- - USN-4448-1
- - USN-4596-1
- - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [debian-lts-announce] 20200523 [SECURITY] [DLA 2217-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25329: Apache Tomcat Incomplete fix for CVE-2020-9484
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20200527 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-dev] 20200625 svn commit: r1879208 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210712 svn commit: r1891484 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20200521 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-users] 20200524 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- - [tomee-commits] 20201013 [jira] [Assigned] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Commented] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Created] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Updated] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20210522 [jira] [Closed] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - http://packetstormsecurity.com/files/157924/Apache-Tomcat-CVE-2020-9484-Proof-Of-Concept.html
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- - https://lists.apache.org/thread.html/r77eae567ed829da9012cadb29af17f2df8fa23bf66faf88229857bb1%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200528-0005/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - openSUSE-SU-2020:0711

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-2021-24122 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

CVSSv2:

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

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

References:

- - [announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-dev] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-dev] 20210114 svn commit: r1885488 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomee-dev] 20210114 Re: Releases?
- - [tomee-dev] 20210115 CVE-2021-24122 NTFS Information Disclosure Bug
- - https://lists.apache.org/thread.html/r1595889b083e05986f42b944dc43060d6b083022260b6ea64d2cec52%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210212-0008/
- - https://www.oracle.com//security-alerts/cpujul2021.html

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-2021-25122 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 Information Exposure

CVSSv2:

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

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

References:

- - DSA-4891
- - GLSA-202208-34
- - [announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25122: Apache Tomcat h2c request mix-up
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 RE: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 Re: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210409-0002/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-2021-25329 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

CVSSv2:

- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

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

References:

- - DSA-4891
- - GLSA-202208-34
- - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25329: Apache Tomcat Incomplete fix for CVE-2020-9484
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - https://lists.apache.org/thread.html/rfe62fbf9d4c314f166fe8c668e50e5d9dd882a99447f26f0367474bf%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210409-0002/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:

- - DSA-4952
- - DSA-4986
- - GLSA-202208-34
- - [debian-lts-announce] 20210805 [SECURITY] [DLA 2733-1] tomcat8 security update
- - https://lists.apache.org/thread.html/r59f9ef03929d32120f91f4ea7e6e79edd5688d75d0a9b65fd26d1fe8%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210827-0007/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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 Smuggling')

CVSSv2:

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

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

References:

- - DSA-4952
- - GLSA-202208-34
- - [debian-lts-announce] 20210805 [SECURITY] [DLA 2733-1] tomcat8 security update
- - [tomee-commits] 20210728 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210728 [jira] [Created] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210830 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210913 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210914 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210916 [jira] [Resolved] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10366
- - https://lists.apache.org/thread.html/r612a79269b0d5e5780c62dfd34286a8037232fec0bc6f1a7e60c9381%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210827-0007/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv2:

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

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:

- - DSA-4986
- - [debian-lts-announce] 20210922 [SECURITY] [DLA 2764-1] tomcat8 security update
- - [tomcat-dev] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS
- - [tomcat-users] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS
- - https://lists.apache.org/thread.html/rccdef0349fdf4fb73a4e4403095446d7fe6264e0a58e2df5c6799434%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20211008-0005/

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-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.

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

References:

- - DSA-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - [oss-security] 20220928 CVE-2021-43980: Apache Tomcat: Information disclosure
- - https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.60
- ...

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.

CVSSv2:

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

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:

- - DSA-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - http://packetstormsecurity.com/files/171728/Apache-Tomcat-10.1-Denial-Of-Service.html
- - https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv
- - https://security.netapp.com/advisory/ntap-20220629-0002/
- - https://www.oracle.com/security-alerts/cpujul2022.html

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-2022-34305 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')

CVSSv2:

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

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

References:

- - GLSA-202208-34
- - [oss-security] 20220623 CVE-2022-34305: Apache Tomcat: XSS in examples web application
- - https://lists.apache.org/thread/k04zk0nq6w57m72w5gb0r6z9ryhmvr4k
- - https://security.netapp.com/advisory/ntap-20220729-0006/

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-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.

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

References:

- - https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq
- - https://security.gentoo.org/glsa/202305-37

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-2023-28708 suppress

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

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

References:

- - https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67

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-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.

The vulnerability is limited to the ROOT (default) web application.

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

References:

- - https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20230921-0006/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-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.

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.

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

References:

- - http://www.openwall.com/lists/oss-security/2023/10/10/9
- - https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20231103-0007/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-2023-44487 suppress

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.

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

References:

- - DSA-5521
- - DSA-5522
- - DSA-5540
- - DSA-5549
- - DSA-5558
- - DSA-5570
- - FEDORA-2023-0259c3f26f
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-492b7be466
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-54fadada12
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-7934802344
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-fe53e13b5b
- - GLSA-202311-09
- - [debian-lts-announce] 20231013 [SECURITY] [DLA 3617-1] tomcat9 security update
- - [debian-lts-announce] 20231016 [SECURITY] [DLA 3617-2] tomcat9 regression update
- - [debian-lts-announce] 20231016 [SECURITY] [DLA 3621-1] nghttp2 security update
- - [debian-lts-announce] 20231030 [SECURITY] [DLA 3641-1] jetty9 security update
- - [debian-lts-announce] 20231031 [SECURITY] [DLA 3638-1] h2o security update
- - [debian-lts-announce] 20231105 [SECURITY] [DLA 3645-1] trafficserver security update
- - [debian-lts-announce] 20231119 [SECURITY] [DLA 3656-1] netty security update
- - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231018 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231018 Vulnerability in Jenkins
- - [oss-security] 20231019 CVE-2023-45802: Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST
- - [oss-security] 20231020 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - https://access.redhat.com/security/cve/cve-2023-44487
- - https://arstechnica.com/security/2023/10/how-ddosers-used-the-http-2-protocol-to-deliver-attacks-of-unprecedented-size/
- - https://aws.amazon.com/security/security-bulletins/AWS-2023-011/
- - https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
- - https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/
- - https://blog.litespeedtech.com/2023/10/11/rapid-reset-http-2-vulnerablilty/
- - https://blog.qualys.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-reset-attack
- - https://blog.vespa.ai/cve-2023-44487/
- - https://bugzilla.proxmox.com/show_bug.cgi?id=4988
- - https://bugzilla.redhat.com/show_bug.cgi?id=2242803
- - https://bugzilla.suse.com/show_bug.cgi?id=1216123
- - https://cgit.freebsd.org/ports/commit/?id=c64c329c2c1752f46b73e3e6ce9f4329be6629f9
- - https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/
- - https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
- - https://community.traefik.io/t/is-traefik-vulnerable-to-cve-2023-44487/20125
- - https://discuss.hashicorp.com/t/hcsec-2023-32-vault-consul-and-boundary-affected-by-http-2-rapid-reset-denial-of-service-vulnerability-cve-2023-44487/59715
- - https://edg.io/lp/blog/resets-leaks-ddos-and-the-tale-of-a-hidden-cve
- - https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764
- - https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131c66a0c088
- - https://github.com/Azure/AKS/issues/3947
- - https://github.com/Kong/kong/discussions/11741

- - https://github.com/advisories/GHSA-qppj-fm5r-hxr3
- - https://github.com/advisories/GHSA-vx74-f528-fxqg
- - https://github.com/advisories/GHSA-xpw8-rcwv-8f8p
- - https://github.com/akka/akka-http/issues/4323
- - https://github.com/alibaba/tengine/issues/1872
- - https://github.com/apache/apisix/issues/10320
- - https://github.com/apache/httpd-site/pull/10
- - https://github.com/apache/httpd/blob/afcdbeebbff4b0c50ea26cdd16e178c0d1f24152/modules/http2/h2_mplx.c#L1101-L1113
- - https://github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2
- - https://github.com/apache/trafficserver/pull/10564
- - https://github.com/arkrwn/PoC/tree/main/CVE-2023-44487
- - https://github.com/bcdannyboy/CVE-2023-44487
- - https://github.com/caddyserver/caddy/issues/5877
- - https://github.com/caddyserver/caddy/releases/tag/v2.7.5
- - https://github.com/dotnet/announcements/issues/277
- - https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73
- - https://github.com/eclipse/jetty.project/issues/10679
- - https://github.com/envoyproxy/envoy/pull/30055
- - https://github.com/etcd-io/etcd/issues/16740
- - https://github.com/facebook/proxygen/pull/466
- - https://github.com/golang/go/issues/63417
- - https://github.com/grpc/grpc-go/pull/6703
- - https://github.com/h2o/h2o/pull/3291
- - https://github.com/h2o/h2o/security/advisories/GHSA-2m7v-gc89-fjqf
- - https://github.com/haproxy/haproxy/issues/2312
- - https://github.com/icing/mod_h2/blob/0a864782af0a942aa2ad4ed960a6b32cd35bcf0a/mod_http2/README.md?plain=1#L239-L244
- - https://github.com/junkurihara/rust-rpxy/issues/97
- - https://github.com/kazu-yamamoto/http2/commit/f61d41a502bd0f60eb24e1ce14edc7b6df6722a1
- - https://github.com/kazu-yamamoto/http2/issues/93
- - https://github.com/kubernetes/kubernetes/pull/121120
- - https://github.com/line/armeria/pull/5232
- - https://github.com/linkerd/website/pull/1695/commits/4b9c6836471bc8270ab48aae6fd2181bc73fd632
- - https://github.com/micrictor/http2-rst-stream
- - https://github.com/microsoft/CBL-Mariner/pull/6381
- - https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820042a285c5e61
- - https://github.com/nghttp2/nghttp2/pull/1961
- - https://github.com/nghttp2/nghttp2/releases/tag/v1.57.0
- - https://github.com/ninenines/cowboy/issues/1615
- - https://github.com/nodejs/node/pull/50121
- - https://github.com/openresty/openresty/issues/930
- - https://github.com/opensearch-project/data-prepper/issues/3474
- - https://github.com/oqtane/oqtane.framework/discussions/3367
- - https://github.com/projectcontour/contour/pull/5826
- - https://github.com/tempesta-tech/tempesta/issues/1986
- - https://github.com/varnishcache/varnish-cache/issues/3996
- - https://groups.google.com/g/golang-announce/c/iNNxDTCjZvo
- - https://istio.io/latest/news/security/istio-security-2023-004/
- - https://linkerd.io/2023/10/12/linkerd-cve-2023-44487/
- - https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q
- - https://lists.w3.org/Archives/Public/ietf-http-wg/2023OctDec/0025.html
- - https://mailman.nginx.org/pipermail/nginx-devel/2023-October/S36Q5HBXR7CAIMPLLPRSSSYR4PCMWILK.html
- - https://martinthomson.github.io/h2-stream-limits/draft-thomson-httpbis-h2-stream-limits.html
- - https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/
- - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487
- - https://my.f5.com/manage/s/article/K000137106
- - https://netty.io/news/2023/10/10/4-1-100-Final.html
- - https://news.ycombinator.com/item?id=37830987
- - https://news.ycombinator.com/item?id=37830998
- - https://news.ycombinator.com/item?id=37831062
- - https://news.ycombinator.com/item?id=37837043
- - https://openssf.org/blog/2023/10/10/http-2-rapid-reset-vulnerability-highlights-need-for-rapid-response/
- - https://seanmonstar.com/post/730794151136935936/hyper-http2-rapid-reset-unaffected
- - https://security.netapp.com/advisory/ntap-20231016-0001/
- - https://security.netapp.com/advisory/ntap-20240426-0007/
- - https://security.netapp.com/advisory/ntap-20240621-0006/
- - https://security.netapp.com/advisory/ntap-20240621-0007/
- - https://security.paloaltonetworks.com/CVE-2023-44487
- - https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14
- - https://ubuntu.com/security/CVE-2023-44487
- - https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/
- - https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487
- - https://www.darkreading.com/cloud/internet-wide-zero-day-bug-fuels-largest-ever-ddos-event
- - https://www.haproxy.com/blog/haproxy-is-not-affected-by-the-http-2-rapid-reset-attack-cve-2023-44487
- - https://www.netlify.com/blog/netlify-successfully-mitigates-cve-2023-44487/
- - https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/
- - https://www.openwall.com/lists/oss-security/2023/10/10/6
- - https://www.phoronix.com/news/HTTP2-Rapid-Reset-Attack
- - https://www.theregister.com/2023/10/10/http2_rapid_reset_zeroday/
- - https://www.vicarius.io/vsociety/posts/rapid-reset-cve-2023-44487-dos-in-http2-understanding-the-root-cause

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-2023-45648 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.

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.

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

References:
- - http://www.openwall.com/lists/oss-security/2023/10/10/10
- - https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20231103-0007/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-2023-46589 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.

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 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

References:
- - https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr
- - https://lists.debian.org/debian-lts-announce/2024/01/msg00001.html
- - https://security.netapp.com/advisory/ntap-20231214-0009/
- - https://www.openwall.com/lists/oss-security/2023/11/28/2

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-2024-21733 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.

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

References:
- - http://packetstormsecurity.com/files/176951/Apache-Tomcat-8.5.63-9.0.43-HTTP-Response-Smuggling.html
- - http://www.openwall.com/lists/oss-security/2024/01/19/2
- - https://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz
- - https://security.netapp.com/advisory/ntap-20240216-0005/

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-2024-38286 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. Older, unsupported versions may also be affected.

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.

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:
- - http://www.openwall.com/lists/oss-security/2024/09/23/2
- - https://lists.apache.org/thread/wms60cvbsz3fpbz9psxtfx8r41jl6d4s

- - https://security.netapp.com/advisory/ntap-20241101-0010/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.13; versions up to (excluding) 9.0.90
- ...

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: /Users/iancoxon/.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

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-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 Smuggling')

CVSSv2:
- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:
- - DSA-4673
- - DSA-4680
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [tomcat-announce] 20200224 [SECURITY] CVE-2019-17569 HTTP Request Smuggling
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - https://security.netapp.com/advisory/ntap-20200327-0005/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345

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-2020-11996 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

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

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:

- - DSA-4727
- - USN-4596-1
- - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release17.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release18.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch trunk updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200701 [jira] [Reopened] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Comment Edited] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20210301 [jira] [Updated] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-users] 20201008 Is Tomcat7 supports HTTP2
- - https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200709-0002/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:1051
- - openSUSE-SU-2020:1063

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 Improper Release of Memory Before Removing Last Reference ('Memory Leak'), CWE-476 NULL Pointer Dereference

CVSSv2:

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

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:

- - DSA-4727
- - USN-4596-1
- - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- - [tomcat-dev] 20200818 [Bug 64671] HTTP/2 Stream.receivedData method throwing continuous NullPointerException in the logs
- - https://lists.apache.org/thread.html/r61f411cf82488d6ec213063fc15feeeb88e31b0ca9c29652ee4f962e%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200724-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:1102
- - openSUSE-SU-2020:1111

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-2020-13935 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')

CVSSv2:

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

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:

- - DSA-4727
- - USN-4448-1
- - USN-4596-1
- - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- - [tomcat-users] 20201118 Re: Strange crash-on-takeoff, Tomcat 7.0.104
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- - https://lists.apache.org/thread.html/rd48c72bd3255bda87564d4da3791517c074d94f8a701f93b85752651%40%3Cannounce.tomcat.apache.org%3E

- - https://security.netapp.com/advisory/ntap-20200724-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - openSUSE-SU-2020:1102
- - openSUSE-SU-2020:1111

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-2020-13943 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

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

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

References:
- - DSA-4835
- - [debian-lts-announce] 20201014 [SECURITY] [DLA 2407-1] tomcat8 security update
- - https://lists.apache.org/thread.html/r4a390027eb27e4550142fac6c8317cc684b157ae314d31514747f307%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20201016-0007/
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - openSUSE-SU-2020:1799
- - openSUSE-SU-2020:1842

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*
- ...

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 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

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

References:
- - DSA-4835
- - GLSA-202012-23
- - [announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [debian-lts-announce] 20201216 [SECURITY] [DLA 2495-1] tomcat8 security update
- - [guacamole-issues] 20201206 [jira] [Commented] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- - [guacamole-issues] 20201206 [jira] [Created] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- - [oss-security] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-dev] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-dev] 20201203 svn commit: r1884073 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210114 svn commit: r1885488 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-users] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomcat-users] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- - [tomee-commits] 20201207 [jira] [Assigned] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - [tomee-commits] 20201207 [jira] [Created] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - [tomee-commits] 20210319 [jira] [Updated] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- - https://lists.apache.org/thread.html/rce5ac9a40173651d540babce59f6f3825f12c6d4e886ba00823b11e5%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20201210-0003/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html

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-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 Smuggling')

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:

- - DSA-4673
- - DSA-4680
- - USN-4448-1
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1935 HTTP Request Smuggling
- - [tomcat-dev] 20210428 [Bug 65272] Problems proccessing HTTP request without CR in last versions
- - [tomcat-users] 20200724 CVE-2020-1935
- - [tomcat-users] 20200724 RE: CVE-2020-1935
- - [tomcat-users] 20200724 Re: CVE-2020-1935
- - [tomcat-users] 20200726 Re: CVE-2020-1935
- - [tomcat-users] 20200727 RE: CVE-2020-1935
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - https://security.netapp.com/advisory/ntap-20200327-0005/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345

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-2020-1938 suppress

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

CVSSv2:

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

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

References:

- - DSA-4673
- - DSA-4680
- - FEDORA-2020-04ac174fa9
- - FEDORA-2020-0e42878ba7
- - FEDORA-2020-c870aa8378
- - GLSA-202003-43
- - [announce] 20210125 Apache Software Foundation Security Report: 2020
- - [announce] 20210223 Re: Apache Software Foundation Security Report: 2020
- - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- - [httpd-bugs] 20200319 [Bug 53098] mod_proxy_ajp: patch to set worker secret passed to tomcat
- - [ofbiz-commits] 20200227 [ofbiz-plugins] branch release17.12 updated: Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938) (OFBIZ-11407)
- - [ofbiz-notifications] 20200225 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200225 [jira] [Updated] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200227 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Comment Edited] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-dev] 20200304 Re: Tagging 10.0.x, 9.0.x, 8.5.x
- - [tomcat-dev] 20200309 [Bug 64206] Answer file not being used

- - [tomcat-dev] 20200625 svn commit: r1879208 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20200301 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200302 AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200304 Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Aw: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Re: Aw: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200309 Re: Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check)
- - [tomcat-users] 20200310 Aw: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200310 Re: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200413 RE: Alternatives for AJP
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2789) TomEE plus is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200320 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Resolved] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-dev] 20200311 CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200311 Re: CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200316 RE: CVE-2020-8840 on TomEE 8.0.1
- - [tomee-users] 20200723 Re: TomEE on Docker
- - http://support.blackberry.com/kb/articleDetail?articleNumber=000062739
- - https://security.netapp.com/advisory/ntap-20200226-0002/
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - openSUSE-SU-2020:0345
- - openSUSE-SU-2020:0597

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-2020-8022 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

CVSSv2:

- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

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

References:

- - [axis-java-dev] 20210228 axis2 1.7.9 is exposed to CVE-2020-8022 via tomcat dependency
- - [axis-java-dev] 20210307 Re: axis2 1.7.9 is exposed to CVE-2020-8022 via tomcat dependency
- - [tomcat-users] 20200902 Re: regarding CVE-2020-8022 applicable to tomcat 8.5.57
- - [tomcat-users] 20200902 regarding CVE-2020-8022 applicable to tomcat 8.5.57
- - https://bugzilla.suse.com/show_bug.cgi?id=1172405
- - openSUSE-SU-2020:0911

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions up to (excluding) 9.0.35-3.57.3
- ...

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

CVSSv2:

- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

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

References:

- - 20200602 [CVE-2020-9484] Apache Tomcat RCE via PersistentManager

- - DSA-4727
- - FEDORA-2020-ce396e7d5c
- - FEDORA-2020-d9169235a8
- - GLSA-202006-21
- - USN-4448-1
- - USN-4596-1
- - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [debian-lts-announce] 20200523 [SECURITY] [DLA 2217-1] tomcat7 security update
- - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25329: Apache Tomcat Incomplete fix for CVE-2020-9484
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20200527 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-dev] 20200625 svn commit: r1879208 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-dev] 20210712 svn commit: r1891484 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20200521 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-users] 20200524 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- - [tomee-commits] 20201013 [jira] [Assigned] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Commented] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Created] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20201013 [jira] [Updated] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - [tomee-commits] 20210522 [jira] [Closed] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- - http://packetstormsecurity.com/files/157924/Apache-Tomcat-CVE-2020-9484-Proof-Of-Concept.html
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- - https://lists.apache.org/thread.html/r77eae567ed829da9012cadb29af17f2df8fa23bf66faf88229857bb1%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20200528-0005/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2020.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2020.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- - openSUSE-SU-2020:0711

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-2021-24122 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

CVSSv2:

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

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

References:

- - [announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-dev] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomcat-dev] 20210114 svn commit: r1885488 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- - [tomee-dev] 20210114 Re: Releases?
- - [tomee-dev] 20210115 CVE-2021-24122 NTFS Information Disclosure Bug
- - https://lists.apache.org/thread.html/r1595889b083e05986f42b944dc43060d6b083022260b6ea64d2cec52%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210212-0008/
- - https://www.oracle.com//security-alerts/cpujul2021.html

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-2021-25122 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 Information Exposure

CVSSv2:

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

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

References:

- - DSA-4891
- - GLSA-202208-34
- - [announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25122: Apache Tomcat h2c request mix-up
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 RE: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 Re: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210409-0002/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-2021-25329 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

CVSSv2:

- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

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

References:

- - DSA-4891
- - GLSA-202208-34
- - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- - [oss-security] 20210301 CVE-2021-25329: Apache Tomcat Incomplete fix for CVE-2020-9484
- - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- - [tomcat-users] 20210702 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- - https://lists.apache.org/thread.html/rfe62fbf9d4c314f166fe8c668e50e5d9dd882a99447f26f0367474bf%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210409-0002/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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

CVSSv2:

- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

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

References:

- - DSA-4952

- - DSA-4986
- - GLSA-202208-34
- - [debian-lts-announce] 20210805 [SECURITY] [DLA 2733-1] tomcat8 security update
- - https://lists.apache.org/thread.html/r59f9ef03929d32120f91f4ea7e6e79edd5688d75d0a9b65fd26d1fe8%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210827-0007/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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 Smuggling')

CVSSv2:

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

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

References:

- - DSA-4952
- - GLSA-202208-34
- - [debian-lts-announce] 20210805 [SECURITY] [DLA 2733-1] tomcat8 security update
- - [tomee-commits] 20210728 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210728 [jira] [Created] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210830 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210913 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210914 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - [tomee-commits] 20210916 [jira] [Resolved] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- - https://kc.mcafee.com/corporate/index?page=content&id=SB10366
- - https://lists.apache.org/thread.html/r612a79269b0d5e5780c62dfd34286a8037232fec0bc6f1a7e60c9381%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20210827-0007/
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv2:

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

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:

- - DSA-4986
- - [debian-lts-announce] 20210922 [SECURITY] [DLA 2764-1] tomcat8 security update
- - [tomcat-dev] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS
- - [tomcat-users] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS
- - https://lists.apache.org/thread.html/rccdef0349fdf4fb73a4e4403095446d7fe6264e0a58e2df5c6799434%40%3Cannounce.tomcat.apache.org%3E
- - https://security.netapp.com/advisory/ntap-20211008-0005/

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-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.

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

References:

- - DSA-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - [oss-security] 20220928 CVE-2021-43980: Apache Tomcat: Information disclosure
- - https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.60
- ...

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.

CVSSv2:

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

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:

- - DSA-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - http://packetstormsecurity.com/files/171728/Apache-Tomcat-10.1-Denial-Of-Service.html
- - https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv
- - https://security.netapp.com/advisory/ntap-20220629-0002/
- - https://www.oracle.com/security-alerts/cpujul2022.html

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-2022-34305 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')

CVSSv2:

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

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

References:

- - GLSA-202208-34
- - [oss-security] 20220623 CVE-2022-34305: Apache Tomcat: XSS in examples web application
- - https://lists.apache.org/thread/k04zk0nq6w57m72w5gb0r6z9ryhmvr4k
- - https://security.netapp.com/advisory/ntap-20220729-0006/

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-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.

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

References:

- - https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq
- - https://security.gentoo.org/glsa/202305-37

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-2023-28708 suppress

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

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

References:

- - https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67

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-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.

The vulnerability is limited to the ROOT (default) web application.

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

References:

- - https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20230921-0006/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-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.

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.

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

References:

- - http://www.openwall.com/lists/oss-security/2023/10/10/9
- - https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20231103-0007/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-2023-44487 suppress

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.

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

References:

- - DSA-5521
- - DSA-5522
- - DSA-5540
- - DSA-5549
- - DSA-5558
- - DSA-5570
- - FEDORA-2023-0259c3f26f
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-492b7be466
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4d2fd884ea

- - FEDORA-2023-54fadada12
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-7934802344
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-fe53e13b5b
- - GLSA-202311-09
- - [debian-lts-announce] 20231013 [SECURITY] [DLA 3617-1] tomcat9 security update
- - [debian-lts-announce] 20231016 [SECURITY] [DLA 3617-2] tomcat9 regression update
- - [debian-lts-announce] 20231016 [SECURITY] [DLA 3621-1] nghttp2 security update
- - [debian-lts-announce] 20231030 [SECURITY] [DLA 3641-1] jetty9 security update
- - [debian-lts-announce] 20231031 [SECURITY] [DLA 3638-1] h2o security update
- - [debian-lts-announce] 20231105 [SECURITY] [DLA 3645-1] trafficserver security update
- - [debian-lts-announce] 20231119 [SECURITY] [DLA 3656-1] netty security update
- - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231018 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231018 Vulnerability in Jenkins
- - [oss-security] 20231019 CVE-2023-45802: Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST
- - [oss-security] 20231020 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - https://access.redhat.com/security/cve/cve-2023-44487
- - https://arstechnica.com/security/2023/10/how-ddosers-used-the-http-2-protocol-to-deliver-attacks-of-unprecedented-size/
- - https://aws.amazon.com/security/security-bulletins/AWS-2023-011/
- - https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
- - https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/
- - https://blog.litespeedtech.com/2023/10/11/rapid-reset-http-2-vulnerablilty/
- - https://blog.qualys.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-reset-attack
- - https://blog.vespa.ai/cve-2023-44487/
- - https://bugzilla.proxmox.com/show_bug.cgi?id=4988
- - https://bugzilla.redhat.com/show_bug.cgi?id=2242803
- - https://bugzilla.suse.com/show_bug.cgi?id=1216123
- - https://cgit.freebsd.org/ports/commit/?id=c64c329c2c1752f46b73e3e6ce9f4329be6629f9
- - https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/
- - https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
- - https://community.traefik.io/t/is-traefik-vulnerable-to-cve-2023-44487/20125
- - https://discuss.hashicorp.com/t/hcsec-2023-32-vault-consul-and-boundary-affected-by-http-2-rapid-reset-denial-of-service-vulnerability-cve-2023-44487/59715
- - https://edg.io/lp/blog/resets-leaks-ddos-and-the-tale-of-a-hidden-cve
- - https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764
- - https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131c66a0c088
- - https://github.com/Azure/AKS/issues/3947
- - https://github.com/Kong/kong/discussions/11741
- - https://github.com/advisories/GHSA-qppj-fm5r-hxr3
- - https://github.com/advisories/GHSA-vx74-f528-fxqg
- - https://github.com/advisories/GHSA-xpw8-rcwv-8f8p
- - https://github.com/akka/akka-http/issues/4323
- - https://github.com/alibaba/tengine/issues/1872
- - https://github.com/apache/apisix/issues/10320
- - https://github.com/apache/httpd-site/pull/10
- - https://github.com/apache/httpd/blob/afcdbeebbff4b0c50ea26cdd16e178c0d1f24152/modules/http2/h2_mplx.c#L1101-L1113
- - https://github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2
- - https://github.com/apache/trafficserver/pull/10564
- - https://github.com/arkrwn/PoC/tree/main/CVE-2023-44487
- - https://github.com/bcdannyboy/CVE-2023-44487
- - https://github.com/caddyserver/caddy/issues/5877
- - https://github.com/caddyserver/caddy/releases/tag/v2.7.5
- - https://github.com/dotnet/announcements/issues/277
- - https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73
- - https://github.com/eclipse/jetty.project/issues/10679
- - https://github.com/envoyproxy/envoy/pull/30055
- - https://github.com/etcd-io/etcd/issues/16740
- - https://github.com/facebook/proxygen/pull/466
- - https://github.com/golang/go/issues/63417
- - https://github.com/grpc/grpc-go/pull/6703
- - https://github.com/h2o/h2o/pull/3291
- - https://github.com/h2o/h2o/security/advisories/GHSA-2m7v-gc89-fjqf
- - https://github.com/haproxy/haproxy/issues/2312
- - https://github.com/icing/mod_h2/blob/0a864782af0a942aa2ad4ed960a6b32cd35bcf0a/mod_http2/README.md?plain=1#L239-L244
- - https://github.com/junkurihara/rust-rpxy/issues/97
- - https://github.com/kazu-yamamoto/http2/commit/f61d41a502bd0f60eb24e1ce14edc7b6df6722a1
- - https://github.com/kazu-yamamoto/http2/issues/93
- - https://github.com/kubernetes/kubernetes/pull/121120
- - https://github.com/line/armeria/pull/5232
- - https://github.com/linkerd/website/pull/1695/commits/4b9c6836471bc8270ab48aae6fd2181bc73fd632
- - https://github.com/micrictor/http2-rst-stream
- - https://github.com/microsoft/CBL-Mariner/pull/6381
- - https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820042a285c5e61
- - https://github.com/nghttp2/nghttp2/pull/1961
- - https://github.com/nghttp2/nghttp2/releases/tag/v1.57.0
- - https://github.com/ninenines/cowboy/issues/1615
- - https://github.com/nodejs/node/pull/50121
- - https://github.com/openresty/openresty/issues/930
- - https://github.com/opensearch-project/data-prepper/issues/3474
- - https://github.com/oqtane/oqtane.framework/discussions/3367
- - https://github.com/projectcontour/contour/pull/5826

- - https://github.com/tempesta-tech/tempesta/issues/1986
- - https://github.com/varnishcache/varnish-cache/issues/3996
- - https://groups.google.com/g/golang-announce/c/iNNxDTCjZvo
- - https://istio.io/latest/news/security/istio-security-2023-004/
- - https://linkerd.io/2023/10/12/linkerd-cve-2023-44487/
- - https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q
- - https://lists.w3.org/Archives/Public/ietf-http-wg/2023OctDec/0025.html
- - https://mailman.nginx.org/pipermail/nginx-devel/2023-October/S36Q5HBXR7CAIMPLLPRSSSYR4PCMWILK.html
- - https://martinthomson.github.io/h2-stream-limits/draft-thomson-httpbis-h2-stream-limits.html
- - https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/
- - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487
- - https://my.f5.com/manage/s/article/K000137106
- - https://netty.io/news/2023/10/10/4-1-100-Final.html
- - https://news.ycombinator.com/item?id=37830987
- - https://news.ycombinator.com/item?id=37830998
- - https://news.ycombinator.com/item?id=37831062
- - https://news.ycombinator.com/item?id=37837043
- - https://openssf.org/blog/2023/10/10/http-2-rapid-reset-vulnerability-highlights-need-for-rapid-response/
- - https://seanmonstar.com/post/730794151136935936/hyper-http2-rapid-reset-unaffected
- - https://security.netapp.com/advisory/ntap-20231016-0001/
- - https://security.netapp.com/advisory/ntap-20240426-0007/
- - https://security.netapp.com/advisory/ntap-20240621-0006/
- - https://security.netapp.com/advisory/ntap-20240621-0007/
- - https://security.paloaltonetworks.com/CVE-2023-44487
- - https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14
- - https://ubuntu.com/security/CVE-2023-44487
- - https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/
- - https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487
- - https://www.darkreading.com/cloud/internet-wide-zero-day-bug-fuels-largest-ever-ddos-event
- - https://www.haproxy.com/blog/haproxy-is-not-affected-by-the-http-2-rapid-reset-attack-cve-2023-44487
- - https://www.netlify.com/blog/netlify-successfully-mitigates-cve-2023-44487/
- - https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/
- - https://www.openwall.com/lists/oss-security/2023/10/10/6
- - https://www.phoronix.com/news/HTTP2-Rapid-Reset-Attack
- - https://www.theregister.com/2023/10/10/http2_rapid_reset_zeroday/
- - https://www.vicarius.io/vsociety/posts/rapid-reset-cve-2023-44487-dos-in-http2-understanding-the-root-cause

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-2023-45648 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.

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.

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

References:

- - http://www.openwall.com/lists/oss-security/2023/10/10/10
- - https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp
- - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- - https://security.netapp.com/advisory/ntap-20231103-0007/
- - https://www.debian.org/security/2023/dsa-5521
- - https://www.debian.org/security/2023/dsa-5522

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-2023-46589 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.

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 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

References:

- - https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr
- - https://lists.debian.org/debian-lts-announce/2024/01/msg00001.html
- - https://security.netapp.com/advisory/ntap-20231214-0009/
- - https://www.openwall.com/lists/oss-security/2023/11/28/2

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-2024-21733 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.

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

References:
- - http://packetstormsecurity.com/files/176951/Apache-Tomcat-8.5.63-9.0.43-HTTP-Response-Smuggling.html
- - http://www.openwall.com/lists/oss-security/2024/01/19/2
- - https://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz
- - https://security.netapp.com/advisory/ntap-20240216-0005/

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-2024-38286 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. Older, unsupported versions may also be affected.

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.

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:
- - http://www.openwall.com/lists/oss-security/2024/09/23/2
- - https://lists.apache.org/thread/wms60cvbsz3fpbz9psxtfx8r41jl6d4s
- - https://security.netapp.com/advisory/ntap-20241101-0010/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.13; versions up to (excluding) 9.0.90
- ...

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the NPM Public Advisories.
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.