How to read the report | **Suppressing false positives** | **Getting Help: github issues**

Sponsor

Project: todolist

th.ab.demo:todolist:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 6.5.3
- *Report Generated On*: Sat, 21 Jun 2025 12:36:57 GMT
- *Dependencies Scanned*: 71 (49 unique)
- *Vulnerable Dependencies*: 18
- *Vulnerabilities Found*: 125
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidenc
h2-1.4.200.jar	cpe:2.3:a:h2database:h2:1.4.200:*:*:*:*:*:*:*	pkg:maven/com.h2database/h2@1.4.200	CRITICAL	5	Highest
jackson-core-2.13.1.jar	cpe:2.3:a:fasterxml:jackson-modules-java8:2.13.1:*:*:*:*:*:*:* cpe:2.3:a:json-java_project:json-java:2.13.1:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-core@2.13.1	HIGH	2	Low
jackson-databind-2.13.1.jar	cpe:2.3:a:fasterxml:jackson-databind:2.13.1:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.13.1:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.13.1	HIGH	4	Highest
jaxb-runtime-2.3.5.jar	cpe:2.3:a:eclipse:glassfish:2.3.5:*:*:*:*:*:*:*	pkg:maven/org.glassfish.jaxb/jaxb-runtime@2.3.5	MEDIUM	1	Highest
logback-classic-1.2.10.jar	cpe:2.3:a:qos:logback:1.2.10:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-classic@1.2.10	HIGH	1	Highest
logback-core-1.2.10.jar	cpe:2.3:a:qos:logback:1.2.10:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.10	HIGH	3	Highest
snakeyaml-1.29.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.29:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.29	CRITICAL	7	Highest
spring-boot-2.6.3.jar	cpe:2.3:a:vmware:spring_boot:2.6.3:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.6.3	CRITICAL	2	Highest
spring-boot-devtools-2.6.3.jar	cpe:2.3:a:vmware:spring_boot:2.6.3:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_boot_tools:2.6.3:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_tools:2.6.3:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-devtools@2.6.3	CRITICAL	2	Highest
spring-context-5.3.15.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-context@5.3.15	CRITICAL	13	Highest
spring-core-5.3.15.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.15	CRITICAL	12	Highest
spring-web-5.3.15.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.15:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.3.15	CRITICAL	17	Highest
spring-webmvc-5.3.15.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.15:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.3.15	CRITICAL	13	Highest
thymeleaf-3.0.14.RELEASE.jar	cpe:2.3:a:thymeleaf:thymeleaf:3.0.14:release:*:*:*:*:*:*	pkg:maven/org.thymeleaf/thymeleaf@3.0.14.RELEASE	HIGH	1	Highest
thymeleaf-extras-java8time-3.0.4.RELEASE.jar	cpe:2.3:a:thymeleaf:thymeleaf:3.0.4:release:*:*:*:*:*:* cpe:2.3:a:time_project:time:3.0.4:release:*:*:*:*:*:*	pkg:maven/org.thymeleaf.extras/thymeleaf-extras-java8time@3.0.4.RELEASE	HIGH	1	Highest
tomcat-embed-core-9.0.56.jar	cpe:2.3:a:apache:tomcat:9.0.56:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.56	CRITICAL	21	Highest
tomcat-embed-websocket-9.0.56.jar	cpe:2.3:a:apache:tomcat:9.0.56:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.56	CRITICAL	19	Highest
txw2-2.3.5.jar	cpe:2.3:a:eclipse:glassfish:2.3.5:*:*:*:*:*:*:*	pkg:maven/org.glassfish.jaxb/txw2@2.3.5	MEDIUM	1	Highest

Dependencies

h2-1.4.200.jar

Description:

H2 Database Engine

License:

MPL 2.0 or EPL 1.0: https://h2database.com/html/license.html

File Path: /root/.m2/repository/com/h2database/h2/1.4.200/h2-1.4.200.jar
MD5: 18c05829a03b92c0880f22a3c4d1d11d
SHA1: f7533fe7cb8e99c87a43d325a77b4b678ad9031a
SHA256:3ad9ac4b6aae9cd9d3ac1c447465e1ed06019b851b893dd6a8d76ddb6d85bca6
Referenced In Project/Scope:todolist:runtime

Evidence

Identifiers

- pkg:maven/com.h2database/h2@1.4.200 (*Confidence*:High)
- cpe:2.3:a:h2database:h2:1.4.200:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2018-14335 (OSSINDEX) suppress

h2database - Improper Link Resolution Before File Access

The software attempts to access a file based on the filename, but it does not properly prevent that filename from identifying a link or shortcut that resolves to an unintended resource.

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:
- Base Score: MEDIUM (6.0)
- Vector: /AV:L/AC:L/Au:/C:H/I:N/A:N

References:
- OSSINDEX - [CVE-2018-14335] CWE-59: Improper Link Resolution Before File Access ('Link Following')
- OSSIndex - https://github.com/h2database/h2database/issues/1294

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:com.h2database:h2:1.4.200:*:*:*:*:*:*:*

CVE-2021-23463 suppress

The package com.h2database:h2 from 1.4.198 and before 2.0.202 are vulnerable to XML External Entity (XXE) Injection via the org.h2.jdbc.JdbcSQLXML class object, when it receives parsed string data from org.h2.jdbc.JdbcResultSet.getSQLXML() method. If it executes the getSource() method when the parameter is DOMSource.class it will trigger the vulnerability.

CWE-611 Improper Restriction of XML External Entity Reference ('XXE')

CVSSv2:
- Base Score: MEDIUM (6.4)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSSv3:
- Base Score: CRITICAL (9.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

References:
- - https://github.com/h2database/h2database/commit/d83285fd2e48fb075780ee95badee6f5a15ea7f8%23diff-008c2e4462609982199cd83e7cf6f1d6b41296b516783f6752c44b9f15dc7bc3
- - https://github.com/h2database/h2database/issues/3195
- - https://github.com/h2database/h2database/pull/3199
- - https://security.netapp.com/advisory/ntap-20230818-0010/
- - https://snyk.io/vuln/SNYK-JAVA-COMH2DATABASE-1769238
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-23463] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
- OSSIndex - https://github.com/h2database/h2database/issues/3195
- OSSIndex - https://github.com/h2database/h2database/pull/3199

Vulnerable Software & Versions:

- cpe:2.3:a:h2database:h2:*:*:*:*:*:*:*:* versions from (including) 1.4.198; versions up to (excluding) 2.0.202

CVE-2021-42392 suppress

The org.h2.util.JdbcUtils.getConnection method of the H2 database takes as parameters the class name of the driver and URL of the database. An attacker may pass a JNDI driver name and a URL leading to a LDAP or RMI servers, causing remote code execution. This can be exploited through various attack vectors, most notably through the H2 Console which leads to unauthenticated remote code execution.

CWE-502 Deserialization of Untrusted Data

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

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-5076
- - [debian-lts-announce] 20220215 [SECURITY] [DLA 2923-1] h2database security update
- - https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6
- - https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/
- - https://security.netapp.com/advisory/ntap-20220119-0001/
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.secpod.com/blog/log4shell-critical-remote-code-execution-vulnerability-in-h2database-console/
- OSSINDEX - [CVE-2021-42392] CWE-502: Deserialization of Untrusted Data
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42392
- OSSIndex - https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:h2database:h2:*:*:*:*:*:*:*:* versions from (including) 1.1.000; versions up to (including) 2.0.204
- ...

CVE-2022-23221 suppress

H2 Console before 2.1.210 allows remote attackers to execute arbitrary code via a jdbc:h2:mem JDBC URL containing the IGNORE_UNKNOWN_SETTINGS=TRUE;FORBID_CREATION=FALSE;INIT=RUNSCRIPT substring, a different vulnerability than CVE-2021-42392.

CWE-88 Argument Injection or Modification

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

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:
- - 20220124 Unauthenticated RCE vuln in the H2 Database console: CVE-2022-23221.
- - DSA-5076
- - [debian-lts-announce] 20220215 [SECURITY] [DLA 2923-1] h2database security update
- - http://packetstormsecurity.com/files/165676/H2-Database-Console-Remote-Code-Execution.html
- - https://github.com/h2database/h2database/releases/tag/version-2.1.210
- - https://github.com/h2database/h2database/security/advisories
- - https://security.netapp.com/advisory/ntap-20230818-0011/
- - https://twitter.com/d0nkey_man/status/1483824727936450564
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- OSSINDEX - [CVE-2022-23221] CWE-88: Argument Injection or Modification
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23221
- OSSIndex - https://github.com/advisories/GHSA-45hx-wfhj-473x
- OSSIndex - https://github.com/h2database/h2database/releases/tag/version-2.1.210
- OSSIndex - https://seclists.org/fulldisclosure/2022/Jan/39

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:h2database:h2:*:*:*:*:*:*:*:* versions from (including) 1.1.100; versions up to (excluding) 2.0.206
- ...

CVE-2022-45868 suppress

The web-based admin console in H2 Database Engine before 2.2.220 can be started via the CLI with the argument -webAdminPassword, which allows the user to specify the password in cleartext for the web admin console. Consequently, a local user (or an attacker that has obtained local access through some means) would be able to discover the password by listing processes and their arguments. NOTE: the vendor states "This is not a vulnerability of H2 Console ... Passwords should never be passed on the command line and every qualified DBA or system administrator is expected to know that." Nonetheless, the issue was fixed in 2.2.220.

CWE-312 Cleartext Storage of Sensitive Information

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/advisories/GHSA-22wj-vf5f-wrvj
- - https://github.com/h2database/h2database/blob/96832bf5a97cdc0adc1f2066ed61c54990d66ab5/h2/src/main/org/h2/server/web/WebServer.java#L346-L347
- - https://github.com/h2database/h2database/issues/3686
- - https://github.com/h2database/h2database/pull/3833
- - https://github.com/h2database/h2database/releases/tag/version-2.2.220
- - https://sites.google.com/sonatype.com/vulnerabilities/sonatype-2022-6243
- OSSINDEX - [CVE-2022-45868] CWE-200: Information Exposure
- OSSIndex - https://github.com/advisories/GHSA-22wj-vf5f-wrvj

Vulnerable Software & Versions:

- cpe:2.3:a:h2database:h2:*:*:*:*:*:*:*:* versions up to (including) 2.1.214

jackson-core-2.13.1.jar

Description:

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

License:

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

File Path: /root/.m2/repository/com/fasterxml/jackson/core/jackson-core/2.13.1/jackson-core-2.13.1.jar
MD5: b5cf9290dc96e215e77f274794d5238e
SHA1: 51ae921a2ed1e06ca8876f12f32f265e83c0b2b8
SHA256:8be6935cd8f9673ac684a589aaa1caecd57dee7c37ed1443d17924325799003d
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/com.fasterxml.jackson.core/jackson-core@2.13.1 (*Confidence*:High)
- cpe:2.3:a:fasterxml:jackson-modules-java8:2.13.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:json-java_project:json-java:2.13.1:*:*:*:*:*:*:* (*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-2.13.1.jar

Description:

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

License:

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

File Path: /root/.m2/repository/com/fasterxml/jackson/core/jackson-databind/2.13.1/jackson-databind-2.13.1.jar
MD5: 15699c52197c95cd66fb722ac93fc07c
SHA1: 698b2d2b15d9a1b7aae025f1d9f576842285e7f6
SHA256:56cfbdc9e1736b5c56b43757f6cf546ee6d49393c79383c4e495c4f7047cb506
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.13.1 (*Confidence*:High)
- cpe:2.3:a:fasterxml:jackson-databind:2.13.1:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:fasterxml:jackson-modules-java8:2.13.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

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 from (including) 2.13.0; versions up to (excluding) 2.13.2.1
- ...

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 from (including) 2.13.0; versions up to (excluding) 2.13.4.1
- ...

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 from (including) 2.13.0; versions up to (excluding) 2.13.4
- ...

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

jaxb-runtime-2.3.5.jar

Description:

JAXB (JSR 222) Reference Implementation

License:

http://www.eclipse.org/org/documents/edl-v10.php

File Path: /root/.m2/repository/org/glassfish/jaxb/jaxb-runtime/2.3.5/jaxb-runtime-2.3.5.jar
MD5: 2d3790292a30333a14b7fb1143864a9c
SHA1: a169a961a2bb9ac69517ec1005e451becf5cdfab
SHA256:4a25453756d08be89c6537cc26fea237677ab99eea857ce1bcb84346715cfae4
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.glassfish.jaxb/jaxb-runtime@2.3.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:glassfish:2.3.5:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2024-9329 suppress

In Eclipse Glassfish versions before 7.0.17, The Host HTTP parameter could cause the web application to redirect to the specified URL, when the requested endpoint is '/management/domain'. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

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

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- - https://github.com/eclipse-ee4j/glassfish/pull/25106
- - https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/232
- - https://www.gruppotim.it/it/footer/red-team.html

Vulnerable Software & Versions:

- cpe:2.3:a:eclipse:glassfish:*:*:*:*:*:*:*:* versions up to (excluding) 7.0.17

logback-classic-1.2.10.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: /root/.m2/repository/ch/qos/logback/logback-classic/1.2.10/logback-classic-1.2.10.jar
MD5: 98021917df75e0a36d0398f7352e5e4f
SHA1: f69d97ef3335c6ab82fc21dfb77ac613f90c1221
SHA256:3160ae988af82c8bf3024ddbe034a82da98bb186fd09e76c50543c5b9da5cc5e
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/ch.qos.logback/logback-classic@1.2.10 (*Confidence*:High)
- cpe:2.3:a:qos:logback:1.2.10:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-6378 suppress

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

CWE-502 Deserialization of Untrusted Data

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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-1.2.10.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: /root/.m2/repository/ch/qos/logback/logback-core/1.2.10/logback-core-1.2.10.jar
MD5: 697b37f140ce9ac35a4ca3eaf4059f1a
SHA1: 5328406bfcae7bcdcc86810fcb2920d2c297170d
SHA256:ba51a3fe56691f9dd7fe742e4a73c3ab4aaaa32202c73409ba56f18687399a08
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/ch.qos.logback/logback-core@1.2.10 (*Confidence*:High)
- cpe:2.3:a:qos:logback:1.2.10:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-6378 suppress

A serialization vulnerability in logback receiver component part of
logback version 1.4.11 allows an attacker to mount a Denial-Of-Service

attack by sending poisoned data.

CWE-502 Deserialization of Untrusted Data

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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:1.2.10:*:*:*:*:*:*:*

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:1.2.10:*:*:*:*:*:*:*

snakeyaml-1.29.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: /root/.m2/repository/org/yaml/snakeyaml/1.29/snakeyaml-1.29.jar
MD5: 5bdf841bc5abda0507fa5ce91c44cc86
SHA1: 6d0cdafb2010f1297e574656551d7145240f6e25
SHA256:89c5f029811b08c878f0b81dbb05e9626624c1fda4087a26871101e499a217ab
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.yaml/snakeyaml@1.29 (*Confidence*:High)
- cpe:2.3:a:snakeyaml_project:snakeyaml:1.29:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-1471 suppress

SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's 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://confluence.atlassian.com/security/cve-2022-1471-snakeyaml-library-rce-vulnerability-in-multiple-products-1296171009.html
- - 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://infosecwriteups.com/%EF%B8%8F-inside-the-160-comment-fight-to-fix-snakeyamls-rce-default-1a20c5ca4d4c
- - 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-2.6.3.jar

Description:

Spring Boot

License:

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

File Path: /root/.m2/repository/org/springframework/boot/spring-boot/2.6.3/spring-boot-2.6.3.jar
MD5: 1a5f70d41966f945bc361b36024c27d1
SHA1: f1127e8a70ba7b9f12581e79ea963b739059bf55
SHA256:33781652e93968fb9b7c6c0856018f42de6aa212b6abce3e3bbc1840c195446f
Referenced In Project/Scope:todolist:compile

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.springframework.boot/spring-boot@2.6.3 (*Confidence*:High)
- cpe:2.3:a:vmware:spring_boot:2.6.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-20873 suppress

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

NVD-CWE-noinfo

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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 from (including) 2.6.0; versions up to (excluding) 2.6.14
- ...

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
- OSSINDEX - [CVE-2023-20883] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20883
- OSSIndex - https://github.com/spring-projects/spring-boot/issues/35552
- OSSIndex - https://spring.io/security/cve-2023-20883

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_boot:*:*:*:*:*:*:*:* versions from (including) 2.6.0; versions up to (including) 2.6.14
- ...

spring-boot-devtools-2.6.3.jar

Description:

Spring Boot Developer Tools

License:

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

File Path: /root/.m2/repository/org/springframework/boot/spring-boot-devtools/2.6.3/spring-boot-devtools-2.6.3.jar
MD5: a5446fb0c3f46b402e6434bb2db99c62
SHA1: 7edce31138c468a256b458ba93ed34cae83e1591
SHA256:898ec10041359a4ad651378e5fb7e56307053652726e68ea8388897e43546667
Referenced In Project/Scope:todolist:runtime

Evidence

Identifiers

- pkg:maven/org.springframework.boot/spring-boot-devtools@2.6.3 (*Confidence*:High)
- cpe:2.3:a:vmware:spring_boot:2.6.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_boot_tools:2.6.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_tools:2.6.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-20873 suppress

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

NVD-CWE-noinfo

CVSSv3:

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

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 from (including) 2.6.0; versions up to (excluding) 2.6.14
- ...

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
- OSSINDEX - [CVE-2023-20883] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20883
- OSSIndex - https://github.com/spring-projects/spring-boot/issues/35552
- OSSIndex - https://spring.io/security/cve-2023-20883

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_boot:*:*:*:*:*:*:*:* versions from (including) 2.6.0; versions up to (including) 2.6.14
- ...

spring-context-5.3.15.jar

Description:

Spring Context

License:

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

File Path: /root/.m2/repository/org/springframework/spring-context/5.3.15/spring-context-5.3.15.jar
MD5: e0019df4d26c3c8e6611bba881808be6
SHA1: 80a12b7dcb3332fbd65c3649249fd35561ffc561
SHA256:b23c4e897e846750d6409982c077f237074534df51eae0e2c589c9783950bf7b
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.springframework/spring-context@5.3.15 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* (*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
- 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:

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

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 from (including) 5.3.0; versions up to (excluding) 5.3.17
- ...

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
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.18
- ...

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
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.18
- ...

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 from (including) 5.3.0; versions up to (including) 5.3.19
- ...

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) 5.3.0; versions up to (including) 5.3.19
- ...

CVE-2023-20860 suppress

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.

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:H/A:N

References:
- - https://security.netapp.com/advisory/ntap-20230505-0006/
- - https://spring.io/security/cve-2023-20860
- OSSINDEX - [CVE-2023-20860] CWE-noinfo
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20860
- OSSIndex - https://spring.io/security/cve-2023-20860

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.26
- ...

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.25
- ...

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) 5.3.0; versions up to (excluding) 5.3.27
- ...

CVE-2024-22259 suppress

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

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

References:
- - https://security.netapp.com/advisory/ntap-20240524-0002/
- - https://spring.io/security/cve-2024-22259

Vulnerable Software & Versions: (show all)

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

CVE-2024-38808 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.

References:
- - https://security.netapp.com/advisory/ntap-20240920-0002/
- - https://spring.io/security/cve-2024-38808
- 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: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.39
- ...

CVE-2024-38820 suppress

The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.

NVD-CWE-noinfo

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-20241129-0003/
- - https://spring.io/security/cve-2024-38820

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.41
- ...

CVE-2025-22233 (OSSINDEX) suppress

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

Affected Spring Products and Versions

Spring Framework:
* 6.2.0 - 6.2.6

* 6.1.0 - 6.1.19

* 6.0.0 - 6.0.27

* 5.3.0 - 5.3.42
* Older, unsupported versions are also affected

Mitigation

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

Affected version(s)Fix Version Availability 6.2.x
6.2.7
OSS6.1.x
6.1.20
OSS6.0.x
6.0.28
Commercial https://enterprise.spring.io/ 5.3.x
5.3.43
Commercial https://enterprise.spring.io/
No further mitigation steps are necessary.

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

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

Credit

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

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

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: LOW (2.3)
- Vector: /AV:N/AC:H/Au:/C:/I:/A:

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

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-context:5.3.15:*:*:*:*:*:*:*

spring-core-5.3.15.jar

Description:

Spring Core

License:

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

File Path: /root/.m2/repository/org/springframework/spring-core/5.3.15/spring-core-5.3.15.jar
MD5: 41f9d7d4f895f401cb9a461a424164d6
SHA1: e813c2311465672d3089fc7be8dbbadb04e64d6b
SHA256:cf3cb24e0f051e338159ad4a60e156d34b082422a80ece3f045bbc6e8c6246ea
Referenced In Project/Scope:todolist:compile

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.springframework/spring-core@5.3.15 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* (*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

- 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:

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

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 from (including) 5.3.0; versions up to (excluding) 5.3.17
- ...

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
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.18
- ...

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
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity

- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.18
- ...

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 from (including) 5.3.0; versions up to (including) 5.3.19
- ...

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) 5.3.0; versions up to (including) 5.3.19
- ...

CVE-2023-20860 suppress

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.

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:H/A:N

References:
- - https://security.netapp.com/advisory/ntap-20230505-0006/
- - https://spring.io/security/cve-2023-20860
- OSSINDEX - [CVE-2023-20860] CWE-noinfo
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20860
- OSSIndex - https://spring.io/security/cve-2023-20860

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.26
- ...

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.25
- ...

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) 5.3.0; versions up to (excluding) 5.3.27
- ...

CVE-2024-22259 suppress

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

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

References:
- - https://security.netapp.com/advisory/ntap-20240524-0002/
- - https://spring.io/security/cve-2024-22259

Vulnerable Software & Versions: (show all)

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

CVE-2024-38808 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.

References:
- - https://security.netapp.com/advisory/ntap-20240920-0002/
- - https://spring.io/security/cve-2024-38808
- 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: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.39
- ...

CVE-2024-38820 suppress

The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.

NVD-CWE-noinfo

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-20241129-0003/
- - https://spring.io/security/cve-2024-38820

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.41
- ...

spring-web-5.3.15.jar

Description:

Spring Web

License:

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

File Path: /root/.m2/repository/org/springframework/spring-web/5.3.15/spring-web-5.3.15.jar
MD5: b6af1ab69cba2deb7e9beb0377ff1bd3
SHA1: a228b373eff7fe34e868827ab02c91b8bf7a643e
SHA256:4c11dbe95c40703d6e55a72c5a1f884f4ffd2b4eb72f8d9cfa3912827aa9f215
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.springframework/spring-web@5.3.15 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:web_project:web:5.3.15:*:*:*:*:*:*:* (*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
- 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:

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

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 from (including) 5.3.0; versions up to (excluding) 5.3.17
- ...

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
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.18
- ...

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
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.18
- ...

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 from (including) 5.3.0; versions up to (including) 5.3.19
- ...

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) 5.3.0; versions up to (including) 5.3.19
- ...

CVE-2023-20860 suppress

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.

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:H/A:N

References:
- - https://security.netapp.com/advisory/ntap-20230505-0006/
- - https://spring.io/security/cve-2023-20860
- OSSINDEX - [CVE-2023-20860] CWE-noinfo
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20860
- OSSIndex - https://spring.io/security/cve-2023-20860

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.26
- ...

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.25
- ...

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) 5.3.0; versions up to (excluding) 5.3.27
- ...

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:5.3.15:*:*:*:*:*:*:*

CVE-2024-22259 suppress

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

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

References:
- - https://security.netapp.com/advisory/ntap-20240524-0002/
- - https://spring.io/security/cve-2024-22259

Vulnerable Software & Versions: (show all)

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

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:5.3.15:*:*:*:*:*:*:*

CVE-2024-38808 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.

References:
- - https://security.netapp.com/advisory/ntap-20240920-0002/
- - https://spring.io/security/cve-2024-38808
- 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: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.39
- ...

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:5.3.15:*:*:*:*:*:*:*

CVE-2024-38820 suppress

The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.

NVD-CWE-noinfo

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-20241129-0003/
- - https://spring.io/security/cve-2024-38820

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.41
- ...

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:5.3.15:*:*:*:*:*:*:*

CVE-2025-41234 (OSSINDEX) suppress

Description

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

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

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

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

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

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

Affected Spring Products and VersionsSpring Framework:

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

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

Affected version(s)Fix versionAvailability6.2.x6.2.8OSS6.1.x6.1.21OSS6.0.x6.0.29 Commercial https://enterprise.spring.io/ No further mitigation steps are necessary.

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

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

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

CVSSv2:
- Base Score: HIGH (7.4)
- Vector: /AV:N/AC:H/Au:/C:/I:/A:

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

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-web:5.3.15:*:*:*:*:*:*:*

spring-webmvc-5.3.15.jar

Description:

Spring Web MVC

License:

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

File Path: /root/.m2/repository/org/springframework/spring-webmvc/5.3.15/spring-webmvc-5.3.15.jar
MD5: 27ed9038864324bbc1100b70df150b03
SHA1: 28307dda4cb5fbeb6f7d7e7c846f464da0eba955
SHA256:77ee2f3d7ff5eef47e15937033de6c478c84bb40a3b90405645f03780dcd9fe1
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.springframework/spring-webmvc@5.3.15 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.3.15:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:web_project:web:5.3.15:*:*:*:*:*:*:* (*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
- 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:

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

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 from (including) 5.3.0; versions up to (excluding) 5.3.17
- ...

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
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.18
- ...

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
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.18
- ...

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 from (including) 5.3.0; versions up to (including) 5.3.19
- ...

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) 5.3.0; versions up to (including) 5.3.19
- ...

CVE-2023-20860 suppress

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.

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:H/A:N

References:
- - https://security.netapp.com/advisory/ntap-20230505-0006/
- - https://spring.io/security/cve-2023-20860
- OSSINDEX - [CVE-2023-20860] CWE-noinfo
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20860
- OSSIndex - https://spring.io/security/cve-2023-20860

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.26
- ...

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (including) 5.3.25
- ...

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) 5.3.0; versions up to (excluding) 5.3.27
- ...

CVE-2024-22259 suppress

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

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

References:
- - https://security.netapp.com/advisory/ntap-20240524-0002/
- - https://spring.io/security/cve-2024-22259

Vulnerable Software & Versions: (show all)

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

CVE-2024-38808 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.

References:
- - https://security.netapp.com/advisory/ntap-20240920-0002/
- - https://spring.io/security/cve-2024-38808
- 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: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.39
- ...

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:5.3.15:*:*:*:*:*:*:*

CVE-2024-38820 suppress

The fix for CVE-2022-22968 made disallowedFields patterns in DataBinder case insensitive. However, String.toLowerCase() has some Locale dependent exceptions that could potentially result in fields not protected as expected.

NVD-CWE-noinfo

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-20241129-0003/
- - https://spring.io/security/cve-2024-38820

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.41
- ...

thymeleaf-3.0.14.RELEASE.jar

Description:

Modern server-side Java template engine for both web and standalone environments

License:

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

File Path: /root/.m2/repository/org/thymeleaf/thymeleaf/3.0.14.RELEASE/thymeleaf-3.0.14.RELEASE.jar
MD5: a8c7b9ae46eb161d763e26761b84db60
SHA1: 05ec84717bf76bcbcc133f9f19bab754f97b92f8
SHA256:30871e0ce3177a984c273878440188aa55fb28aa1742e148136ce2fe04017053
Referenced In Project/Scope:todolist:compile

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.thymeleaf/thymeleaf@3.0.14.RELEASE (*Confidence*:High)
- cpe:2.3:a:thymeleaf:thymeleaf:3.0.14:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-38286 suppress

Thymeleaf through 3.1.1.RELEASE, as used in spring-boot-admin (aka Spring Boot Admin) through 3.1.1 and other products, allows sandbox bypass via crafted HTML. This may be relevant for SSTI (Server Side Template Injection) and code execution in spring-boot-admin if MailNotifier is enabled and there is write access to environment variables via the UI.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- - https://github.com/p1n93r/SpringBootAdmin-thymeleaf-SSTI
- OSSINDEX - [CVE-2023-38286] CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-38286
- OSSIndex - https://github.com/p1n93r/SpringBootAdmin-thymeleaf-SSTI
- OSSIndex - https://github.com/thymeleaf/thymeleaf/issues/966

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:thymeleaf:thymeleaf:*:*:*:*:*:*:*:* versions up to (including) 3.1.1
- ...

thymeleaf-extras-java8time-3.0.4.RELEASE.jar

Description:

Modern server-side Java template engine for both web and standalone environments

License:

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

File Path: /root/.m2/repository/org/thymeleaf/extras/thymeleaf-extras-java8time/3.0.4.RELEASE/thymeleaf-extras-java8time-3.0.4.RELEASE.jar
MD5: 01420fcda7481663f967836c440f9bc5
SHA1: 36e7175ddce36c486fff4578b5af7bb32f54f5df
SHA256:c07690c764329afd148a4134980d636911390a3fda45f6c6ae46517e4b4444d3
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.thymeleaf.extras/thymeleaf-extras-java8time@3.0.4.RELEASE (*Confidence*:High)
- cpe:2.3:a:thymeleaf:thymeleaf:3.0.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:time_project:time:3.0.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2023-38286 suppress

Thymeleaf through 3.1.1.RELEASE, as used in spring-boot-admin (aka Spring Boot Admin) through 3.1.1 and other products, allows sandbox bypass via crafted HTML. This may be relevant for SSTI (Server Side Template Injection) and code execution in spring-boot-admin if MailNotifier is enabled and there is write access to environment variables via the UI.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- - https://github.com/p1n93r/SpringBootAdmin-thymeleaf-SSTI

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:thymeleaf:thymeleaf:*:*:*:*:*:*:*:* versions up to (including) 3.1.1
- ...

tomcat-embed-core-9.0.56.jar

Description:

Core Tomcat implementation

License:

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

File Path: /root/.m2/repository/org/apache/tomcat/embed/tomcat-embed-core/9.0.56/tomcat-embed-core-9.0.56.jar
MD5: 4a9b9d1046f040407d8fcb2badb6a908
SHA1: 7c8e0008564c644beec976ab115e2670bb4d7003
SHA256:17d020617f6be1b792ff4a7516ae71b0928ea73e0d9845f13c244d95d015f5fa
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.56 (*Confidence*:High)
- cpe:2.3:a:apache:tomcat:9.0.56:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

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-2022-23181 suppress

The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.

CVSSv2:
- Base Score: LOW (3.7)
- Vector: /AV:L/AC:H/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-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - https://lists.apache.org/thread/l8x62p3k19yfcb208jo4zrb83k5mfwg9
- - https://security.netapp.com/advisory/ntap-20220217-0010/
- - 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:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.35; versions up to (including) 9.0.56
- ...

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/2b4qmhbcygvc7dyfpjyx54c03x65vhcv
- - 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/k04zk0ng6w57m72w5gb0r6z9ryhmvr4k
- - 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.

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/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-2022-45143 suppress

The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.

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/yqkd183xrw3wqvnpcg3osbcryq85fkzj
- - https://security.gentoo.org/glsa/202305-37
- - https://security.netapp.com/advisory/ntap-20230216-0009/
- OSSINDEX - [CVE-2022-45143] CWE-116: Improper Encoding or Escaping of Output
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-45143
- OSSIndex - https://github.com/todobugs/tomcat/pull/2
- OSSIndex - https://github.com/todobugs/tomcat/pull/3
- OSSIndex - https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj
- OSSIndex - https://tomcat.apache.org/security-10.html
- OSSIndex - https://tomcat.apache.org/security-8.html
- OSSIndex - https://tomcat.apache.org/security-9.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.40; versions up to (excluding) 9.0.69
- ...

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-2023-0259c3f26f
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-492b7be466
- - FEDORA-2023-492b7be466
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-54fadada12
- - FEDORA-2023-54fadada12
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-7934802344
- - FEDORA-2023-7934802344
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-fe53e13b5b
- - 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] 20231010 CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231010 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] 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-vulnerablility/
- - 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/grpc/grpc/releases/tag/v1.59.2
- 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http2-reset-d8Kf32vZ
- 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/2023/10/6
- 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-2024-23672 suppress

Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

References:
- - http://www.openwall.com/lists/oss-security/2024/03/13/4
- - https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f
- - https://lists.debian.org/debian-lts-announce/2024/04/msg00001.html
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
- - https://security.netapp.com/advisory/ntap-20240402-0002/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.86
- ...

CVE-2024-24549 suppress

Denial of Service due to improper input validation vulnerability for HTTP/2 requests in Apache Tomcat. When processing an HTTP/2 request, if the request exceeded any of the configured limits for headers, the associated HTTP/2 stream was not reset until after all of the headers had been processed.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

NVD-CWE-noinfo

References:
- - http://www.openwall.com/lists/oss-security/2024/03/13/3
- - https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg
- - https://lists.debian.org/debian-lts-announce/2024/04/msg00001.html
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
- - https://security.netapp.com/advisory/ntap-20240402-0002/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.86
- ...

CVE-2024-34750 suppress

Improper Handling of Exceptional Conditions, Uncontrolled Resource Consumption vulnerability in Apache Tomcat. When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.0-M1 through 9.0.89.

Users are recommended to upgrade to version 11.0.0-M21, 10.1.25 or 9.0.90, which fixes the issue.

References:
- - https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l
- - https://security.netapp.com/advisory/ntap-20240816-0004/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.90
- ...

CVE-2024-38286 suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. 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
- ...

CVE-2024-52316 suppress

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

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95.

Users are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fix the issue.

CWE-754 Improper Check for Unusual or Exceptional Conditions

References:
- - http://www.openwall.com/lists/oss-security/2024/11/18/2
- - https://lists.apache.org/thread/lopzlqh91jj9n334g02om08sbysdb928
- - https://security.netapp.com/advisory/ntap-20250124-0003/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.96
- ...

CVE-2025-24813 suppress

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.

If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:
- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads
- attacker knowledge of the names of security sensitive files being uploaded
- the security sensitive files also being uploaded via partial PUT

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

Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- - http://www.openwall.com/lists/oss-security/2025/03/10/5
- - https://github.com/absholi7ly/POC-CVE-2025-24813/blob/main/README.md
- - https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
- - https://lists.debian.org/debian-lts-announce/2025/04/msg00003.html
- - https://security.netapp.com/advisory/ntap-20250321-0001/
- - https://www.vicarius.io/vsociety/posts/cve-2025-24813-detect-apache-tomcat-rce
- - https://www.vicarius.io/vsociety/posts/cve-2025-24813-mitigate-apache-tomcat-rce

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (excluding) 9.0.99
- ...

CVE-2025-31651 suppress

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. For a subset of unlikely rewrite rule configurations, it was possible for a specially crafted request to bypass some rewrite rules. If those
rewrite rules effectively enforced security constraints, those
constraints could be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.5, from 10.1.0-M1 through 10.1.39, from 9.0.0.M1 through 9.0.102.

Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.

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://www.openwall.com/lists/oss-security/2025/04/28/3
- - https://lists.apache.org/list.html?announce@tomcat.apache.org

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.104
- ...

CVE-2025-48988 (OSSINDEX) suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2025-48988 for details

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:
- Base Score: HIGH (8.7)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

References:
- OSSINDEX - [CVE-2025-48988] CWE-770: Allocation of Resources Without Limits or Throttling
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48988
- OSSIndex - https://github.com/advisories/GHSA-h3gc-qfqq-6h8f

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.apache.tomcat.embed:tomcat-embed-core:9.0.56:*:*:*:*:*:*:*

CVE-2025-49125 (OSSINDEX) suppress

Authentication Bypass Using an Alternate Path or Channel vulnerability in Apache Tomcat. When using PreResources or PostResources mounted other than at the root of the web application, it was possible to access those resources via an unexpected path. That path was likely not to be protected by the same security constraints as the expected path, allowing those security constraints to be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105.

Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.

CWE-288 Authentication Bypass Using an Alternate Path or Channel

CVSSv2:
- Base Score: MEDIUM (6.3)
- Vector: /AV:N/AC:L/Au:/C:/I:/A:

References:
- OSSINDEX - [CVE-2025-49125] CWE-288: Authentication Bypass Using an Alternate Path or Channel
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49125
- OSSIndex - https://github.com/advisories/GHSA-wc4r-xq3c-5cf3

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.apache.tomcat.embed:tomcat-embed-core:9.0.56:*:*:*:*:*:*:*

tomcat-embed-websocket-9.0.56.jar

Description:

Core Tomcat implementation

License:

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

File Path: /root/.m2/repository/org/apache/tomcat/embed/tomcat-embed-websocket/9.0.56/tomcat-embed-websocket-9.0.56.jar
MD5: 11ac79336e580aeaaf5fccc8d99e9414
SHA1: d84be683a5d47e820d077db1d511181c7db9e4e9
SHA256:d78145d4d87880e2b0403cad49f41cc289ad2d89be50ca494ae22edd61283e73
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.56 (*Confidence*:High)
- cpe:2.3:a:apache:tomcat:9.0.56:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

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-2022-23181 suppress

The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.

CVSSv2:
- Base Score: LOW (3.7)
- Vector: /AV:L/AC:H/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-5265
- - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- - https://lists.apache.org/thread/l8x62p3k19yfcb208jo4zrb83k5mfwg9
- - https://security.netapp.com/advisory/ntap-20220217-0010/
- - 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:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.35; versions up to (including) 9.0.56
- ...

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/2b4qmhbcygvc7dyfpjyx54c03x65vhcv
- - 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.

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/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-2022-45143 suppress

The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.

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/yqkd183xrw3wqvnpcg3osbcryq85fkzj
- - https://security.gentoo.org/glsa/202305-37
- - https://security.netapp.com/advisory/ntap-20230216-0009/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.40; versions up to (excluding) 9.0.69
- ...

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-2023-0259c3f26f
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-492b7be466
- - FEDORA-2023-492b7be466
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-54fadada12
- - FEDORA-2023-54fadada12
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-7934802344

- - FEDORA-2023-7934802344
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-fe53e13b5b
- - 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] 20231010 CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- - [oss-security] 20231010 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] 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-vulnerablility/
- - 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/grpc/grpc/releases/tag/v1.59.2
- - 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/microctor/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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http2-reset-d8Kf32vZ
- - 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-2024-23672 suppress

Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

References:
- - http://www.openwall.com/lists/oss-security/2024/03/13/4
- - https://lists.apache.org/thread/cmpswfx6lj4s7x0nxxosvfqs11lvdx2f
- - https://lists.debian.org/debian-lts-announce/2024/04/msg00001.html
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
- - https://security.netapp.com/advisory/ntap-20240402-0002/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.86
- ...

CVE-2024-24549 suppress

Denial of Service due to improper input validation vulnerability for HTTP/2 requests in Apache Tomcat. When processing an HTTP/2 request, if the request exceeded any of the configured limits for headers, the associated HTTP/2 stream was not reset until after all of the headers had been processed.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98.

Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.

NVD-CWE-noinfo

References:
- - http://www.openwall.com/lists/oss-security/2024/03/13/3
- - https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg
- - https://lists.debian.org/debian-lts-announce/2024/04/msg00001.html
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/3UWIS5MMGYDZBLJYT674ZI5AWFHDZ46B/
- - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/736G4GPZWS2DSQO5WKXO3G6OMZKFEK55/
- - https://security.netapp.com/advisory/ntap-20240402-0002/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.86
- ...

CVE-2024-34750 suppress

Improper Handling of Exceptional Conditions, Uncontrolled Resource Consumption vulnerability in Apache Tomcat. When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.0-M1 through 9.0.89.

Users are recommended to upgrade to version 11.0.0-M21, 10.1.25 or 9.0.90, which fixes the issue.

References:
- - https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l
- - https://security.netapp.com/advisory/ntap-20240816-0004/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.90
- ...

CVE-2024-38286 suppress

Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. 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
- ...

CVE-2024-52316 suppress

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

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95.

Users are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fix the issue.

CWE-754 Improper Check for Unusual or Exceptional Conditions

References:
- - http://www.openwall.com/lists/oss-security/2024/11/18/2
- - https://lists.apache.org/thread/lopzlqh91jj9n334g02om08sbysdb928
- - https://security.netapp.com/advisory/ntap-20250124-0003/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.96
- ...

CVE-2025-24813 suppress

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.

If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:
- writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads
- attacker knowledge of the names of security sensitive files being uploaded
- the security sensitive files also being uploaded via partial PUT

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

Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

CWE-502 Deserialization of Untrusted Data, CWE-706 Use of Incorrectly-Resolved Name or Reference

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- - http://www.openwall.com/lists/oss-security/2025/03/10/5
- - https://github.com/absholi7ly/POC-CVE-2025-24813/blob/main/README.md
- - https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq
- - https://lists.debian.org/debian-lts-announce/2025/04/msg00003.html
- - https://security.netapp.com/advisory/ntap-20250321-0001/
- - https://www.vicarius.io/vsociety/posts/cve-2025-24813-detect-apache-tomcat-rce
- - https://www.vicarius.io/vsociety/posts/cve-2025-24813-mitigate-apache-tomcat-rce

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (excluding) 9.0.99
- ...

CVE-2025-31651 suppress

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. For a subset of unlikely rewrite rule configurations, it was possible for a specially crafted request to bypass some rewrite rules. If those
rewrite rules effectively enforced security constraints, those
constraints could be bypassed.

This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.5, from 10.1.0-M1 through 10.1.39, from 9.0.0.M1 through 9.0.102.

Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.

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://www.openwall.com/lists/oss-security/2025/04/28/3
- - https://lists.apache.org/list.html?announce@tomcat.apache.org

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.104
- ...

txw2-2.3.5.jar

Description:

TXW is a library that allows you to write XML documents.

File Path: /root/.m2/repository/org/glassfish/jaxb/txw2/2.3.5/txw2-2.3.5.jar
MD5: 67005a4cf5ee9cfd82edec1bdbecb32b
SHA1: ec8930fa62e7b1758b1664d135f50c7abe86a4a3
SHA256:7d75ea1151367fb66287011d9941715f645922932554acba0c5ac3aec67fb01f
Referenced In Project/Scope:todolist:compile

Evidence

Identifiers

- pkg:maven/org.glassfish.jaxb/txw2@2.3.5 (*Confidence*:High)
- cpe:2.3:a:eclipse:glassfish:2.3.5:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2024-9329 suppress

In Eclipse Glassfish versions before 7.0.17, The Host HTTP parameter could cause the web application to redirect to the specified URL, when the requested endpoint is '/management/domain'. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

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

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- - https://github.com/eclipse-ee4j/glassfish/pull/25106
- - https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/232
- - https://www.gruppotim.it/it/footer/red-team.html

Vulnerable Software & Versions:

- cpe:2.3:a:eclipse:glassfish:*:*:*:*:*:*:*:* versions up to (excluding) 7.0.17

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.