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

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 5.3.0
- *Report Generated On*: Fri, 8 Dec 2023 12:44:52 -0900
- *Dependencies Scanned*: 49 (34 unique)
- *Vulnerable Dependencies*: 17
- *Vulnerabilities Found*: 74
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence
spring-boot-starter-data-rest-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_data_rest:2.2.4:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE	CRITICAL	3	Highest
spring-data-rest-webmvc-3.2.4.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_data_rest:3.2.4:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_data_rest:3.2.4:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE	MEDIUM	2	Highest
spring-hateoas-1.0.3.RELEASE.jar	cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE	MEDIUM	1	Highest
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	CRITICAL	3	Highest
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.3	HIGH	2	Highest
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	CRITICAL	5	Highest
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:* cpe:2.3:a:yaml_project:yaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	10	Highest
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL	26	Highest
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	1	Highest
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	HIGH	4	Highest
spring-beans-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE	HIGH	1	Highest
spring-webmvc-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE	MEDIUM	1	Highest
spring-context-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-context@5.2.3.RELEASE	MEDIUM	1	Highest
spring-expression-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE	MEDIUM	3	Highest
json-path-2.4.0.jar	cpe:2.3:a:json-java_project:json-java:2.4.0:*:*:*:*:*:*:*	pkg:maven/com.jayway.jsonpath/json-path@2.4.0	HIGH	2	Low
json-smart-2.3.jar	cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:*	pkg:maven/net.minidev/json-smart@2.3	HIGH	3	Highest

Dependencies

spring-boot-starter-data-rest-2.2.4.RELEASE.jar

Description:

Starter for exposing Spring Data repositories over REST using Spring Data REST

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\boot\spring-boot-starter-data-rest\2.2.4.RELEASE\spring-boot-starter-data-rest-2.2.4.RELEASE.jar
MD5: 829dcdea073775b5df54ff9fb9f01038
SHA1: 8ee304ca3c39cbbde13fc5f785660403241d30d0
SHA256:98fb2311865c7df0da687b78fdc26745c85087e33311e4c46b2e3581ae20aa6d
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

- pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE (*Confidence*:High)
- cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_data_rest:2.2.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-27772 suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- OSSINDEX - [CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere

Vulnerable Software & Versions:

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

CVE-2023-20873 suppress

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

NVD-CWE-noinfo

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2023-20883 suppress

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

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20230703-0008/
- MISC - https://spring.io/security/cve-2023-20883
- OSSINDEX - [CVE-2023-20883] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')

Vulnerable Software & Versions: (show all)

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

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

Description:

Spring Data REST - WebMVC

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\data\spring-data-rest-webmvc\3.2.4.RELEASE\spring-data-rest-webmvc-3.2.4.RELEASE.jar
MD5: da22f3d4eb417e9e0a7ae9a73961c4f0
SHA1: acaae431117245ed5f1d09166207b076bbe3ac82
SHA256:7694c509ffaff229d45630d2ee68525588f80d2740deeef7642696f1440043d1
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2021-22047 (OSSINDEX) suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

CVSSv2:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/C:L/I:N/A:N

References:
- OSSINDEX - [CVE-2021-22047] CWE-668: Exposure of Resource to Wrong Sphere

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2022-31679 (OSSINDEX) suppress

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

CWE-284 Improper Access Control

CVSSv2:
- Base Score: LOW (3.7)
- Vector: /AV:N/AC:H/Au:/C:L/I:N/A:N

References:
- OSSINDEX - [CVE-2022-31679] CWE-284: Improper Access Control

Vulnerable Software & Versions (OSSINDEX):

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

spring-hateoas-1.0.3.RELEASE.jar

Description:

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

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\hateoas\spring-hateoas\1.0.3.RELEASE\spring-hateoas-1.0.3.RELEASE.jar
MD5: efbda177ffbc4a8c7a693080528c9cd8
SHA1: 35c3514a8336d31f346f7b5c99de2f1ee32611ac

SHA256:5a54edfd6ae2e6a85bd694682a358a0a55282f426623da59d47d879de3e1846d
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2023-34036 suppress

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

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

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

CWE-116 Improper Encoding or Escaping of Output

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - https://spring.io/security/cve-2023-34036
- OSSINDEX - [CVE-2023-34036] CWE-116: Improper Encoding or Escaping of Output

Vulnerable Software & Versions: (show all)

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

jackson-databind-2.10.2.jar

Description:

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

License:

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

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

Evidence

Identifiers

- pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2 (*Confidence*:High)
- cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-25649 suppress

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

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

CVSSv2:

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

CVSSv3:

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

References:

- - FEDORA-2021-1d8254899c
- - [druid-commits] 20201208 [GitHub] [druid] jihoonson opened a new pull request #10655: Bump up jackson-databind to 2.10.5.1
- - [flink-issues] 20210121 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- - [flink-issues] 20210122 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- - [hive-dev] 20210223 [jira] [Created] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Assigned] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210223 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210315 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210316 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210503 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210510 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20210514 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20211012 [jira] [Resolved] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [hive-issues] 20211012 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- - [iotdb-commits] 20210325 [iotdb] branch master updated: [IOTDB-1256] upgrade Jackson to 2.11.0 because of loopholes CVE-2020-25649 (#2896)
- - [iotdb-notifications] 20210324 [jira] [Created] (IOTDB-1256) Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 closed pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 opened a new pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [iotdb-reviews] 20210325 [GitHub] [iotdb] jixuan1989 merged pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- - [kafka-dev] 20201215 Re: [VOTE] 2.7.0 RC5
- - [kafka-dev] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- - [kafka-dev] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-dev] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-jira] 20201205 [GitHub] [kafka] sirocchj opened a new pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] ijuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201210 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-jira] 20201215 [GitHub] [kafka] ijuma merged pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- - [kafka-users] 20201215 Re: [VOTE] 2.7.0 RC5
- - [kafka-users] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- - [kafka-users] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [kafka-users] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre commented on pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre merged pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [GitHub] [karaf] svogt opened a new pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [karaf-commits] 20210217 [karaf] branch master updated: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- - [knox-dev] 20210601 [jira] [Created] (KNOX-2614) Upgrade Jackson due to CVE-2020-25649
- - [knox-dev] 20210601 [jira] [Updated] (KNOX-2614) Upgrade jackson-databind to 2.10.5 due to CVE-2020-25649
- - [spark-user] 20210621 Re: CVEs
- - [tomee-commits] 20210127 [jira] [Created] (TOMEE-2965) CVE-2020-25649 - Update jackson databind
- - [turbine-commits] 20210316 svn commit: r1887732 - in /turbine/fulcrum/trunk/json: ./ jackson/ jackson/src/test/org/apache/fulcrum/json/jackson/ jackson2/ jackson2/src/test/org/apache/fulcrum/json/jackson/ jackson2/src/test/org/apache/fulcrum/json/jackson/mixins/
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5.9 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-commits] 20210106 [zookeeper] branch master updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-dev] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210105 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210106 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210106 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-issues] 20210116 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] asfgit closed pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] edwin092 opened a new pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] nkalmar commented on pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- - https://lists.apache.org/thread.html/r31f4ee7d561d56a0c2c2c6eb1d6ce3e05917ff9654fdbfec05dc2b83%40%3Ccommits.servicecomb.apache.org%3E
- CONFIRM - https://security.netapp.com/advisory/ntap-20210108-0007/
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1887664
- MISC - https://github.com/FasterXML/jackson-databind/issues/2589
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- N/A - N/A
- N/A - N/A
- OSSINDEX - [CVE-2020-25649] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:fasterxml:jackson-databind:*:*:*:*:*:*:*:* versions from (including) 2.10.0; versions up to (excluding) 2.10.5.1
- ...

CVE-2020-36518 suppress

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

CWE-787 Out-of-bounds Write

CVSSv2:

- Base Score: MEDIUM (5.0)

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220506-0004/
- DEBIAN - DSA-5283
- MISC - https://github.com/FasterXML/jackson-databind/issues/2816
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MLIST - [debian-lts-announce] 20220502 [SECURITY] [DLA 2990-1] jackson-databind security update
- MLIST - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- N/A - N/A
- OSSINDEX - [CVE-2020-36518] CWE-787: Out-of-bounds Write

Vulnerable Software & Versions: (show all)

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

CVE-2021-46877 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2022-42003 suppress

In FasterXML jackson-databind before 2.14.0-rc1, 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. Additional fix version in 2.13.4.1 and 2.12.17.1

CWE-502 Deserialization of Untrusted Data

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20221124-0004/
- DEBIAN - DSA-5283
- GENTOO - GLSA-202210-21
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020
- MISC - https://github.com/FasterXML/jackson-databind/commit/d78d00ee7b5245b93103fef3187f70543d67ca33
- MISC - https://github.com/FasterXML/jackson-databind/issues/3590
- MLIST - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- OSSINDEX - [CVE-2022-42003] CWE-502: Deserialization of Untrusted Data

Vulnerable Software & Versions: (show all)

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

CVE-2022-42004 suppress

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

CWE-502 Deserialization of Untrusted Data

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20221118-0008/
- DEBIAN - DSA-5283
- GENTOO - GLSA-202210-21
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490
- MISC - https://github.com/FasterXML/jackson-databind/commit/063183589218fec19a9293ed2f17ec53ea80ba88
- MISC - https://github.com/FasterXML/jackson-databind/issues/3582
- MLIST - [debian-lts-announce] 20221127 [SECURITY] [DLA 3207-1] jackson-databind security update
- OSSINDEX - [CVE-2022-42004] CWE-502: Deserialization of Untrusted Data

Vulnerable Software & Versions: (show all)

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

CVE-2023-35116 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv3:
- Base Score: MEDIUM (4.7)
- Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - 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

spring-boot-2.2.4.RELEASE.jar

Description:

Spring Boot

License:

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

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

Evidence

Related Dependencies

Identifiers

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

Published Vulnerabilities

CVE-2022-27772 suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- OSSINDEX - [CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere

Vulnerable Software & Versions:

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

CVE-2023-20873 suppress

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

NVD-CWE-noinfo

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20230601-0009/

- MISC - https://spring.io/blog/2023/05/18/spring-boot-2-5-15-and-2-6-15-available-now
- MISC - https://spring.io/security/cve-2023-20873

Vulnerable Software & Versions: (show all)

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

CVE-2023-20883 suppress

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

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20230703-0008/
- MISC - https://spring.io/security/cve-2023-20883
- OSSINDEX - [CVE-2023-20883] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')

Vulnerable Software & Versions: (show all)

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

logback-core-1.2.3.jar

Description:

logback-core module

License:

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

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

Evidence

Related Dependencies

Identifiers

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

Published Vulnerabilities

CVE-2021-42550 suppress

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

CWE-502 Deserialization of Untrusted Data

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

CVSSv3:
- Base Score: MEDIUM (6.6)
- Vector: /AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

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

Vulnerable Software & Versions: (show all)

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

CVE-2023-6378 suppress

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

CWE-502 Deserialization of Untrusted Data

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: /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
- OSSINDEX - [CVE-2023-6378] CWE-502: Deserialization of Untrusted Data
- OSSINDEX - [CVE-2023-6378] CWE-502: Deserialization of Untrusted Data

Vulnerable Software & Versions: (show all)

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

log4j-api-2.12.1.jar

Description:

The Apache Log4j API

License:

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

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

Evidence

Related Dependencies

Identifiers

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

Published Vulnerabilities

CVE-2020-9488 suppress

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

CWE-295 Improper Certificate Validation

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

CVSSv3:
- Base Score: LOW (3.7)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- - [db-torque-dev] 20200715 Build failed in Jenkins: Torque4-trunk #685
- - [db-torque-dev] 20210127 Re: Items for our (delayed) quarterly report to the board?
- - [db-torque-dev] 20210128 Antwort: Re: Items for our (delayed) quarterly report to the board?
- - [flink-issues] 20210510 [GitHub] [flink] zentol opened a new pull request #15879: [FLINK-22407][build] Bump log4j to 2.24.1
- - [hive-dev] 20201207 [jira] [Created] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-dev] 20210216 [jira] [Created] (HIVE-24787) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Assigned] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201207 [jira] [Work started] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201208 [jira] [Updated] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488
- - [hive-issues] 20201208 [jira] [Work logged] (HIVE-24500) Hive - upgrade log4j 2.12.1 to 2.13.2+ due to CVE-2020-9488

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

Vulnerable Software & Versions: (show all)

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

CVE-2021-44228 suppress

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion'), CWE-502 Deserialization of Untrusted Data, CWE-20 Improper Input Validation

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: CRITICAL (10.0)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References:
- - FEDORA-2021-66d6c484f3
- - FEDORA-2021-f0f501d01f
- CERT-VN - VU#930724
- CISCO - 20211210 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf
- CONFIRM - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032
- CONFIRM - https://security.netapp.com/advisory/ntap-20211210-0007/
- CONFIRM - https://support.apple.com/kb/HT213189
- CONFIRM - https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html
- CONFIRM - https://www.oracle.com/security-alerts/alert-cve-2021-44228.html
- DEBIAN - DSA-5020
- FULLDISC - 20220314 APPLE-SA-2022-03-14-7 Xcode 13.3
- FULLDISC - 20220721 Open-Xchange Security Advisory 2022-07-21
- FULLDISC - 20221208 Intel Data Center Manager <= 5.1 Local Privileges Escalation
- MISC - http://packetstormsecurity.com/files/165225/Apache-Log4j2-2.14.1-Remote-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/165260/VMware-Security-Advisory-2021-0028.html
- MISC - http://packetstormsecurity.com/files/165261/Apache-Log4j2-2.14.1-Information-Disclosure.html
- MISC - http://packetstormsecurity.com/files/165270/Apache-Log4j2-2.14.1-Remote-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/165281/Log4j2-Log4Shell-Regexes.html
- MISC - http://packetstormsecurity.com/files/165282/Log4j-Payload-Generator.html
- MISC - http://packetstormsecurity.com/files/165306/L4sh-Log4j-Remote-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/165307/Log4j-Remote-Code-Execution-Word-Bypassing.html
- MISC - http://packetstormsecurity.com/files/165311/log4j-scan-Extensive-Scanner.html
- MISC - http://packetstormsecurity.com/files/165371/VMware-Security-Advisory-2021-0028.4.html
- MISC - http://packetstormsecurity.com/files/165532/Log4Shell-HTTP-Header-Injection.html
- MISC - http://packetstormsecurity.com/files/165642/VMware-vCenter-Server-Unauthenticated-Log4Shell-JNDI-Injection-Remote-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/165673/UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/167794/Open-Xchange-App-Suite-7.10.x-Cross-Site-Scripting-Command-Injection.html
- MISC - http://packetstormsecurity.com/files/167917/MobileIron-Log4Shell-Remote-Command-Execution.html
- MISC - http://packetstormsecurity.com/files/171626/AD-Manager-Plus-7122-Remote-Code-Execution.html

- MISC - https://github.com/cisagov/log4j-affected-db
- MISC - https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md
- MISC - https://github.com/nu11secur1ty/CVE-mitre/tree/main/CVE-2021-44228
- MISC - https://logging.apache.org/log4j/2.x/security.html
- MISC - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
- MISC - https://twitter.com/kurtseifried/status/1469345530182455296
- MISC - https://www.bentley.com/en/common-vulnerability-exposure/be-2022-0001
- MISC - https://www.nu11secur1ty.com/2021/12/cve-2021-44228.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [debian-lts-announce] 20211212 [SECURITY] [DLA 2842-1] apache-log4j2 security update
- MLIST - [oss-security] 20211210 CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints
- MLIST - [oss-security] 20211210 Re: CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints
- MLIST - [oss-security] 20211210 Re: CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints
- MLIST - [oss-security] 20211213 CVE-2021-4104: Deserialization of untrusted data in JMSAppender in Apache Log4j 1.2
- MLIST - [oss-security] 20211213 Re: CVE-2021-4104: Deserialization of untrusted data in JMSAppender in Apache Log4j 1.2
- MLIST - [oss-security] 20211214 CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
- MLIST - [oss-security] 20211215 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
- MS - Microsoft's Response to CVE-2021-44228 Apache Log4j 2

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* versions from (including) 2.4.0; versions up to (excluding) 2.12.2
- ...

CVE-2021-44832 suppress

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

CWE-20 Improper Input Validation

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

CVSSv3:
- Base Score: MEDIUM (6.6)
- Vector: /AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

References:
- - FEDORA-2021-1bd9151bab
- - FEDORA-2021-c6f471ce0f
- CISCO - 20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf
- CONFIRM - https://security.netapp.com/advisory/ntap-20220104-0001/
- MISC - https://issues.apache.org/jira/browse/LOG4J2-3293
- MISC - https://lists.apache.org/thread/s1o5vlo78ypqxnzn6p8zf6t9shtq5143
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [debian-lts-announce] 20211229 [SECURITY] [DLA 2870-1] apache-log4j2 security update
- MLIST - [oss-security] 20211228 CVE-2021-44832: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* versions from (including) 2.4; versions up to (excluding) 2.12.4
- ...

CVE-2021-45046 suppress

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

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

CVSSv2:
- Base Score: MEDIUM (5.1)
- Vector: /AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.0)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

References:
- CERT-VN - VU#930724
- CISCO - 20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf
- CONFIRM - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032
- CONFIRM - https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html
- CONFIRM - https://www.oracle.com/security-alerts/alert-cve-2021-44228.html
- DEBIAN - DSA-5022
- MISC - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/EOKPQGV24RRBBI4TBZUDQMM4MEH7MXCY/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/SIG7FZULMNK2XF6FZRU4VWYDQXNMUGAJ/
- MISC - https://logging.apache.org/log4j/2.x/security.html
- MISC - https://security.gentoo.org/glsa/202310-16

- MISC - https://www.cve.org/CVERecord?id=CVE-2021-44228
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [oss-security] 20211214 CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
- MLIST - [oss-security] 20211215 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
- MLIST - [oss-security] 20211218 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* versions from (including) 2.0.1; versions up to (excluding) 2.12.2
- ...

CVE-2021-45105 suppress

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

CWE-20 Improper Input Validation, CWE-674 Uncontrolled Recursion

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

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CERT-VN - VU#930724
- CISCO - 20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-501673.pdf
- CONFIRM - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032
- CONFIRM - https://security.netapp.com/advisory/ntap-20211218-0001/
- DEBIAN - DSA-5024
- MISC - https://logging.apache.org/log4j/2.x/security.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.zerodayinitiative.com/advisories/ZDI-21-1541/
- MLIST - [oss-security] 20211218 CVE-2021-45105: Apache Log4j2 does not always protect from infinite recursion in lookup evaluation
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

snakeyaml-1.25.jar

Description:

YAML 1.1 parser and emitter for Java

License:

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

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

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2017-18640 suppress

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

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

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

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

References:
- - FEDORA-2020-23012fafbc
- - FEDORA-2020-599514b47e
- - [atlas-commits] 20200915 [atlas] branch master updated: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)
- - [atlas-commits] 20200916 [atlas] 02/02: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640 (#110)
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab closed pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #109: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200907 [GitHub] [atlas] crazylab opened a new pull request #110: Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [GitHub] [atlas] nixonrodrigues commented on pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [jira] [Created] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200914 [jira] [Updated] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200915 [GitHub] [atlas] nixonrodrigues merged pull request #110: ATLAS-3940 : Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200915 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [atlas-dev] 20200916 [jira] [Commented] (ATLAS-3940) Upgrade snakeyaml to a version without CVE-2017-18640
- - [cassandra-commits] 20200930 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Created] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20200930 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201001 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201002 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201002 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201007 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201007 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [cassandra] branch trunk updated: Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Comment Edited] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Commented] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-commits] 20201009 [jira] [Updated] (CASSANDRA-16150) Upgrade to snakeyaml >= 1.26 version for CVE-2017-18640 fix
- - [cassandra-pr] 20200907 [GitHub] [cassandra] crazylab opened a new pull request #736: Upgrade to a snakeyaml version without CVE
- - [hadoop-common-commits] 20201028 [hadoop] branch branch-3.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20201028 [hadoop] branch trunk updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20211008 [hadoop] branch branch-3.2 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-commits] 20211008 [hadoop] branch branch-3.2.3 updated: HADOOP-17236. Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640. Contributed by Brahma Reddy Battula.
- - [hadoop-common-dev] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200830 [jira] [Created] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200830 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200831 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20200909 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201026 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201027 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201028 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20201028 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211006 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211008 [jira] [Commented] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [hadoop-common-issues] 20211008 [jira] [Updated] (HADOOP-17236) Bump up snakeyaml to 1.26 to mitigate CVE-2017-18640
- - [kafka-users] 20210617 vulnerabilities
- - [phoenix-dev] 20210419 [GitHub] [phoenix-omid] richardantal opened a new pull request #93: OMID-207 Upgrade to snakeyaml 1.26 due to CVE-2017-18640
- - [phoenix-dev] 20210419 [jira] [Created] (OMID-207) Upgrade to snakeyaml 1.26 due to CVE-2017-18640
- - [pulsar-commits] 20200830 [GitHub] [pulsar] codelipenghui commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy commented on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200831 [GitHub] [pulsar] wolfstudy edited a comment on issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - [pulsar-commits] 20200907 [GitHub] [pulsar] jiazhai closed issue #7928: CVE-2017-18640 exposure snakeyaml below 1.26
- - https://lists.apache.org/thread.html/r4c682fb8cf69dd14162439656a6ebdf42ea6ad0e4edba95907ea3f14%40%3Ccommits.servicecomb.apache.org%3E
- - https://lists.apache.org/thread.html/r900e020760c89f082df1c6e0d46320eba721e4e47bb9eb521e68cd95%40%3Ccommits.servicecomb.apache.org%3E
- GENTOO - GLSA-202305-28
- MISC - https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion
- MISC - https://bitbucket.org/asomov/snakeyaml/wiki/Billion%20laughs%20attack
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/377
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/wiki/Changes
- MISC - https://mvnrepository.com/artifact/org.yaml/snakeyaml/1.25/usages
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- OSSINDEX - [CVE-2017-18640] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

Vulnerable Software & Versions: (show all)

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

CVE-2021-4235 suppress

Due to unbounded alias chasing, a maliciously crafted YAML file can cause the system to consume significant system resources. If parsing user input, this may be used as a denial of service vector.

NVD-CWE-noinfo

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: /AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References:
- MISC - https://github.com/go-yaml/yaml/commit/bb4e33bf68bf89cad44d386192cbed201f35b241
- MISC - https://github.com/go-yaml/yaml/pull/375
- MISC - https://lists.debian.org/debian-lts-announce/2023/07/msg00001.html
- MISC - https://pkg.go.dev/vuln/GO-2021-0061

Vulnerable Software & Versions:

- cpe:2.3:a:yaml_project:yaml:*:*:*:*:*:go:*:* versions up to (excluding) 2.2.3

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: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- - http://www.openwall.com/lists/oss-security/2023/11/19/1
- MISC - http://packetstormsecurity.com/files/175095/PyTorch-Model-Server-Registration-Deserialization-Remote-Code-Execution.html
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/561/cve-2022-1471-vulnerability-in#comment-64581479
- MISC - https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2
- MISC - https://github.com/mbechler/marshalsec
- MISC - https://groups.google.com/g/kubernetes-security-announce/c/mwrakFaEdnc
- MISC - https://security.netapp.com/advisory/ntap-20230818-0015/
- MISC - https://www.github.com/mbechler/marshalsec/blob/master/marshalsec.pdf?raw=true
- OSSINDEX - [CVE-2022-1471] CWE-20: Improper Input Validation

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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - N/A
- CONFIRM - N/A
- CONFIRM - N/A
- CONFIRM - N/A
- MLIST - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- OSSINDEX - [CVE-2022-25857] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

Vulnerable Software & Versions:

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

CVE-2022-3064 suppress

Parsing malicious or large YAML documents can consume excessive amounts of CPU or memory.

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

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

References:
- MISC - https://github.com/go-yaml/yaml/commit/f221b8435cfb71e54062f6c6e99e9ade30b124d5
- MISC - https://github.com/go-yaml/yaml/releases/tag/v2.2.4
- MISC - https://lists.debian.org/debian-lts-announce/2023/07/msg00001.html
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4SBIUECMLNC572P23DDOKJNKPJVX26SP/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ANIOPUXWIHVRA6CEWXCGOMX3YYS6KFHG/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LYZOKMMVX4SIEHPJW3SJUQGMO5YZCPHC/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PW3XC47AUW5J5M2ULJX7WCCL3B2ETLMT/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/XNF4OLYZRQE75EB5TW5N42FSXHBXGWFE/
- MISC - https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ZTE4ITXXPIWZEQ4HYQCB6N6GZIMWXDAI/
- MISC - https://pkg.go.dev/vuln/GO-2022-0956

Vulnerable Software & Versions:

- cpe:2.3:a:yaml_project:yaml:*:*:*:*:*:go:*:* versions up to (excluding) 2.2.4

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: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- GENTOO - GLSA-202305-28
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/525/got-stackoverflowerror-for-many-open
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47024
- MLIST - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- OSSINDEX - [CVE-2022-38749] CWE-787: Out-of-bounds Write

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: /AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References:
- GENTOO - GLSA-202305-28
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027
- MLIST - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- OSSINDEX - [CVE-2022-38750] CWE-787: Out-of-bounds Write

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: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- GENTOO - GLSA-202305-28
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039
- MLIST - [debian-lts-announce] 20221002 [SECURITY] [DLA 3132-1] snakeyaml security update
- OSSINDEX - [CVE-2022-38751] CWE-787: Out-of-bounds Write

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: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- GENTOO - GLSA-202305-28
- MISC - https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverflow-oss-fuzz-47081
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081
- OSSINDEX - [CVE-2022-38752] CWE-787: Out-of-bounds Write

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: /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
- CONFIRM - N/A
- OSSINDEX - [CVE-2022-41854] CWE-121: Stack-based Buffer Overflow

Vulnerable Software & Versions:

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

tomcat-embed-core-9.0.30.jar

Description:

Core Tomcat implementation

License:

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

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

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30 (*Confidence*:High)
- cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2019-17569 suppress

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

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

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.28; versions up to (including) 9.0.30
- ...

CVE-2020-11996 suppress

A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.

NVD-CWE-noinfo

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

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

References:
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release17.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch release18.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-commits] 20200628 [ofbiz-framework] branch trunk updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200701 [jira] [Reopened] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)

- - [ofbiz-notifications] 20200703 [jira] [Comment Edited] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200703 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20210301 [jira] [Updated] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-users] 20201008 Is Tomcat7 supports HTTP2
- CONFIRM - https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E
- CONFIRM - https://security.netapp.com/advisory/ntap-20200709-0002/
- DEBIAN - DSA-4727
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- SUSE - openSUSE-SU-2020:1051
- SUSE - openSUSE-SU-2020:1063
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.35
- ...

CVE-2020-13934 suppress

An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.

CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak'), CWE-476 NULL Pointer Dereference

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

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

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.36
- ...

CVE-2020-13935 suppress

The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

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

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

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

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.36
- ...

CVE-2020-13943 suppress

If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-17527 suppress

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

CWE-200 Information Exposure

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

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

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.35
- ...

CVE-2020-1935 suppress

In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

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

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

References:
- - [tomcat-dev] 20210428 [Bug 65272] Problems proccessing HTTP request without CR in last versions
- - [tomcat-users] 20200724 CVE-2020-1935
- - [tomcat-users] 20200724 RE: CVE-2020-1935
- - [tomcat-users] 20200724 Re: CVE-2020-1935
- - [tomcat-users] 20200726 Re: CVE-2020-1935
- - [tomcat-users] 20200727 RE: CVE-2020-1935
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities

- CONFIRM - https://security.netapp.com/advisory/ntap-20200327-0005/
- DEBIAN - DSA-4673
- DEBIAN - DSA-4680
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- MLIST - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- MLIST - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1935 HTTP Request Smuggling
- SUSE - openSUSE-SU-2020:0345
- UBUNTU - USN-4448-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.30
- ...

CVE-2020-1938 suppress

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

NVD-CWE-Other

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

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

References:
- - FEDORA-2020-04ac174fa9
- - FEDORA-2020-0e42878ba7
- - FEDORA-2020-c870aa8378
- - [announce] 20210125 Apache Software Foundation Security Report: 2020
- - [announce] 20210223 Re: Apache Software Foundation Security Report: 2020
- - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- - [httpd-bugs] 20200319 [Bug 53098] mod_proxy_ajp: patch to set worker secret passed to tomcat
- - [ofbiz-commits] 20200227 [ofbiz-plugins] branch release17.12 updated: Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938) (OFBIZ-11407)
- - [ofbiz-notifications] 20200225 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200225 [jira] [Updated] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200227 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Comment Edited] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200228 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- - [tomcat-dev] 20200304 Re: Tagging 10.0.x, 9.0.x, 8.5.x
- - [tomcat-dev] 20200309 [Bug 64206] Answer file not being used
- - [tomcat-dev] 20200625 svn commit: r1879208 - in /tomcat/site/trunk: docs/security-10.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20200301 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200302 AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- - [tomcat-users] 20200302 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- - [tomcat-users] 20200304 Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Aw: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200305 Re: Aw: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200309 Re: Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check)
- - [tomcat-users] 20200310 Aw: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200310 Re: Re: Re: Fix for CVE-2020-1938
- - [tomcat-users] 20200413 RE: Alternatives for AJP
- - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2789) TomEE plus is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200320 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Resolved] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-commits] 20201127 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- - [tomee-dev] 20200311 CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200311 Re: CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- - [tomee-dev] 20200316 RE: CVE-2020-8840 on TomEE 8.0.1
- - [tomee-users] 20200723 Re: TomEE on Docker
- CONFIRM - http://support.blackberry.com/kb/articleDetail?articleNumber=000062739
- CONFIRM - https://security.netapp.com/advisory/ntap-20200226-0002/
- DEBIAN - DSA-4673
- DEBIAN - DSA-4680
- GENTOO - GLSA-202003-43
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- MLIST - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- MLIST - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- SUSE - openSUSE-SU-2020:0345
- SUSE - openSUSE-SU-2020:0597

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.30
- ...

CVE-2020-8022 suppress

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CWE-276 Incorrect Default Permissions

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-9484 suppress

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CWE-502 Deserialization of Untrusted Data

CVSSv2:
- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.0)
- Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

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

- N/A - N/A
- SUSE - openSUSE-SU-2020:0711
- UBUNTU - USN-4448-1
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (excluding) 9.0.43
- ...

CVE-2021-24122 suppress

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CWE-706 Use of Incorrectly-Resolved Name or Reference

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

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.39
- ...

CVE-2021-25122 suppress

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

CWE-200 Information Exposure

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

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

References:
- - [announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-dev] 20210301 svn commit: r1887027 - in /tomcat/site/trunk: docs/security-10.html docs/security-7.html docs/security-8.html docs/security-9.html xdocs/security-10.xml xdocs/security-7.xml xdocs/security-8.xml xdocs/security-9.xml
- - [tomcat-users] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 RE: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- - [tomcat-users] 20210305 Re: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- CONFIRM - N/A
- CONFIRM - https://security.netapp.com/advisory/ntap-20210409-0002/
- DEBIAN - DSA-4891
- GENTOO - GLSA-202208-34
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- MLIST - [oss-security] 20210301 CVE-2021-25122: Apache Tomcat h2c request mix-up
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.41
- ...

CVE-2021-25329 suppress

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.4)
- Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.0)
- Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (including) 9.0.41
- ...

CVE-2021-30640 suppress

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

CWE-116 Improper Encoding or Escaping of Output

CVSSv2:

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

CVSSv3:

- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N

References:

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.46
- ...

CVE-2021-33037 suppress

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

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

CVSSv2:

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

CVSSv3:

- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (excluding) 9.0.0; versions up to (including) 9.0.46
- ...

CVE-2021-41079 suppress

Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

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

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

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

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.44
- ...

CVE-2021-43980 suppress

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

CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CVSSv3:
- Base Score: LOW (3.7)
- Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

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

Vulnerable Software & Versions: (show all)

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

CVE-2022-29885 suppress

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

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

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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220629-0002/
- DEBIAN - DSA-5265
- MISC - http://packetstormsecurity.com/files/171728/Apache-Tomcat-10.1-Denial-Of-Service.html
- MISC - https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv
- MLIST - [debian-lts-announce] 20221026 [SECURITY] [DLA 3160-1] tomcat9 security update
- N/A - N/A

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:N/A:N

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

References:
- CONFIRM - N/A
- CONFIRM - https://security.netapp.com/advisory/ntap-20220729-0006/
- GENTOO - GLSA-202208-34
- MLIST - [oss-security] 20220623 CVE-2022-34305: Apache Tomcat: XSS in examples web application

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 10.1.1 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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

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

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 9.0.68
- ...

CVE-2023-28708 suppress

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

CWE-523 Unprotected Transport of Credentials

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

References:
- MISC - 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.

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

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

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

CWE-459 Incomplete Cleanup

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - http://www.openwall.com/lists/oss-security/2023/10/10/9
- MISC - https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw

- MISC - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- MISC - https://security.netapp.com/advisory/ntap-20231103-0007/
- MISC - https://www.debian.org/security/2023/dsa-5521
- MISC - 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.

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

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

References:
- - DSA-5558
- - DSA-5570
- - FEDORA-2023-0259c3f26f
- - FEDORA-2023-17efd3f2cd
- - FEDORA-2023-1caffb88af
- - FEDORA-2023-2a9214af5f
- - FEDORA-2023-3f70b8d406
- - FEDORA-2023-492b7be466
- - FEDORA-2023-4bf641255e
- - FEDORA-2023-4d2fd884ea
- - FEDORA-2023-54fadada12
- - FEDORA-2023-5ff7bf1dd8
- - FEDORA-2023-7934802344
- - FEDORA-2023-7b52921cae
- - FEDORA-2023-822aab0a5a
- - FEDORA-2023-b2c50535cb
- - FEDORA-2023-c0c6a91330
- - FEDORA-2023-d5030c983c
- - FEDORA-2023-dbe64661af
- - FEDORA-2023-e9c04d81c1
- - FEDORA-2023-ed2642fd58
- - FEDORA-2023-f66fc0f62a
- - FEDORA-2023-fe53e13b5b
- - GLSA-202311-09
- - [debian-lts-announce] 20231119 [SECURITY] [DLA 3656-1] netty security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20231016-0001/
- DEBIAN - DSA-5521
- DEBIAN - DSA-5522
- DEBIAN - DSA-5540
- DEBIAN - DSA-5549
- MISC - https://access.redhat.com/security/cve/cve-2023-44487
- MISC - https://arstechnica.com/security/2023/10/how-ddosers-used-the-http-2-protocol-to-deliver-attacks-of-unprecedented-size/
- MISC - https://aws.amazon.com/security/security-bulletins/AWS-2023-011/
- MISC - https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
- MISC - https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/
- MISC - https://blog.litespeedtech.com/2023/10/11/rapid-reset-http-2-vulnerablilty/
- MISC - https://blog.qualys.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-reset-attack
- MISC - https://blog.vespa.ai/cve-2023-44487/
- MISC - https://bugzilla.proxmox.com/show_bug.cgi?id=4988
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2242803
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=1216123
- MISC - https://cgit.freebsd.org/ports/commit/?id=c64c329c2c1752f46b73e3e6ce9f4329be6629f9
- MISC - https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/
- MISC - https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
- MISC - https://community.traefik.io/t/is-traefik-vulnerable-to-cve-2023-44487/20125
- MISC - 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
- MISC - https://edg.io/lp/blog/resets-leaks-ddos-and-the-tale-of-a-hidden-cve
- MISC - https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764
- MISC - https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131c66a0c088
- MISC - https://github.com/Azure/AKS/issues/3947
- MISC - https://github.com/Kong/kong/discussions/11741
- MISC - https://github.com/advisories/GHSA-qppj-fm5r-hxr3
- MISC - https://github.com/advisories/GHSA-vx74-f528-fxqg
- MISC - https://github.com/advisories/GHSA-xpw8-rcwv-8f8p
- MISC - https://github.com/akka/akka-http/issues/4323
- MISC - https://github.com/alibaba/tengine/issues/1872
- MISC - https://github.com/apache/apisix/issues/10320
- MISC - https://github.com/apache/httpd-site/pull/10
- MISC - https://github.com/apache/httpd/blob/afcdbeebbff4b0c50ea26cdd16e178c0d1f24152/modules/http2/h2_mplx.c#L1101-L1113
- MISC - https://github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2
- MISC - https://github.com/apache/trafficserver/pull/10564
- MISC - https://github.com/arkrwn/PoC/tree/main/CVE-2023-44487
- MISC - https://github.com/bcdannyboy/CVE-2023-44487
- MISC - https://github.com/caddyserver/caddy/issues/5877
- MISC - https://github.com/caddyserver/caddy/releases/tag/v2.7.5
- MISC - https://github.com/dotnet/announcements/issues/277
- MISC - https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73
- MISC - https://github.com/eclipse/jetty.project/issues/10679
- MISC - https://github.com/envoyproxy/envoy/pull/30055
- MISC - https://github.com/etcd-io/etcd/issues/16740
- MISC - https://github.com/facebook/proxygen/pull/466
- MISC - https://github.com/golang/go/issues/63417
- MISC - https://github.com/grpc/grpc-go/pull/6703
- MISC - https://github.com/h2o/h2o/pull/3291

- MISC - https://github.com/h2o/h2o/security/advisories/GHSA-2m7v-gc89-fjqf
- MISC - https://github.com/haproxy/haproxy/issues/2312
- MISC - https://github.com/icing/mod_h2/blob/0a864782af0a942aa2ad4ed960a6b32cd35bcf0a/mod_http2/README.md?plain=1#L239-L244
- MISC - https://github.com/junkurihara/rust-rpxy/issues/97
- MISC - https://github.com/kazu-yamamoto/http2/commit/f61d41a502bd0f60eb24e1ce14edc7b6df6722a1
- MISC - https://github.com/kazu-yamamoto/http2/issues/93
- MISC - https://github.com/kubernetes/kubernetes/pull/121120
- MISC - https://github.com/line/armeria/pull/5232
- MISC - https://github.com/linkerd/website/pull/1695/commits/4b9c6836471bc8270ab48aae6fd2181bc73fd632
- MISC - https://github.com/micrictor/http2-rst-stream
- MISC - https://github.com/microsoft/CBL-Mariner/pull/6381
- MISC - https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820042a285c5e61
- MISC - https://github.com/nghttp2/nghttp2/pull/1961
- MISC - https://github.com/nghttp2/nghttp2/releases/tag/v1.57.0
- MISC - https://github.com/ninenines/cowboy/issues/1615
- MISC - https://github.com/nodejs/node/pull/50121
- MISC - https://github.com/openresty/openresty/issues/930
- MISC - https://github.com/opensearch-project/data-prepper/issues/3474
- MISC - https://github.com/oqtane/oqtane.framework/discussions/3367
- MISC - https://github.com/projectcontour/contour/pull/5826
- MISC - https://github.com/tempesta-tech/tempesta/issues/1986
- MISC - https://github.com/varnishcache/varnish-cache/issues/3996
- MISC - https://groups.google.com/g/golang-announce/c/iNNxDTCjZvo
- MISC - https://istio.io/latest/news/security/istio-security-2023-004/
- MISC - https://linkerd.io/2023/10/12/linkerd-cve-2023-44487/
- MISC - https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q
- MISC - https://lists.w3.org/Archives/Public/ietf-http-wg/2023OctDec/0025.html
- MISC - https://mailman.nginx.org/pipermail/nginx-devel/2023-October/S36Q5HBXR7CAIMPLLPRSSSYR4PCMWILK.html
- MISC - https://martinthomson.github.io/h2-stream-limits/draft-thomson-httpbis-h2-stream-limits.html
- MISC - https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/
- MISC - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44487
- MISC - https://my.f5.com/manage/s/article/K000137106
- MISC - https://netty.io/news/2023/10/10/4-1-100-Final.html
- MISC - https://news.ycombinator.com/item?id=37830987
- MISC - https://news.ycombinator.com/item?id=37830998
- MISC - https://news.ycombinator.com/item?id=37831062
- MISC - https://news.ycombinator.com/item?id=37837043
- MISC - https://openssf.org/blog/2023/10/10/http-2-rapid-reset-vulnerability-highlights-need-for-rapid-response/
- MISC - https://seanmonstar.com/post/730794151136935936/hyper-http2-rapid-reset-unaffected
- MISC - https://security.paloaltonetworks.com/CVE-2023-44487
- MISC - https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14
- MISC - https://ubuntu.com/security/CVE-2023-44487
- MISC - https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/
- MISC - https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487
- MISC - https://www.darkreading.com/cloud/internet-wide-zero-day-bug-fuels-largest-ever-ddos-event
- MISC - https://www.haproxy.com/blog/haproxy-is-not-affected-by-the-http-2-rapid-reset-attack-cve-2023-44487
- MISC - https://www.netlify.com/blog/netlify-successfully-mitigates-cve-2023-44487/
- MISC - https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/
- MISC - https://www.openwall.com/lists/oss-security/2023/10/10/6
- MISC - https://www.phoronix.com/news/HTTP2-Rapid-Reset-Attack
- MISC - https://www.theregister.com/2023/10/10/http2_rapid_reset_zeroday/
- MLIST - [debian-lts-announce] 20231013 [SECURITY] [DLA 3617-1] tomcat9 security update
- MLIST - [debian-lts-announce] 20231016 [SECURITY] [DLA 3617-2] tomcat9 regression update
- MLIST - [debian-lts-announce] 20231016 [SECURITY] [DLA 3621-1] nghttp2 security update
- MLIST - [debian-lts-announce] 20231030 [SECURITY] [DLA 3641-1] jetty9 security update
- MLIST - [debian-lts-announce] 20231031 [SECURITY] [DLA 3638-1] h2o security update
- MLIST - [debian-lts-announce] 20231105 [SECURITY] [DLA 3645-1] trafficserver security update
- MLIST - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- MLIST - [oss-security] 20231013 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- MLIST - [oss-security] 20231018 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
- MLIST - [oss-security] 20231018 Vulnerability in Jenkins
- MLIST - [oss-security] 20231019 CVE-2023-45802: Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST
- MLIST - [oss-security] 20231020 Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations

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.

CWE-20 Improper Input Validation

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - http://www.openwall.com/lists/oss-security/2023/10/10/10
- MISC - https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp
- MISC - https://lists.debian.org/debian-lts-announce/2023/10/msg00020.html
- MISC - https://security.netapp.com/advisory/ntap-20231103-0007/
- MISC - https://www.debian.org/security/2023/dsa-5521
- MISC - 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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- - https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr
- - 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
- ...

hibernate-validator-6.0.18.Final.jar

Description:

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

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\hibernate\validator\hibernate-validator\6.0.18.Final\hibernate-validator-6.0.18.Final.jar
MD5: d3eeb4f1bf013d939b86dfc34b0c6a5d
SHA1: 7fd00bcd87e14b6ba66279282ef15efa30dd2492
SHA256:79fb11445bc48e1ea6fb259e825d58b3c9a5fa2b7e3c9527e41e4aeda82de907
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-10693 suppress

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

CWE-20 Improper Input Validation

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- - [portals-pluto-dev] 20210714 [jira] [Created] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-791 Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2020-10693] CWE-20: Improper Input Validation

Vulnerable Software & Versions: (show all)

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

spring-web-5.2.3.RELEASE.jar

Description:

Spring Web

License:

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

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

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2016-1000027 (OSSINDEX) suppress

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

CWE-502 Deserialization of Untrusted Data

CVSSv2:
- Base Score: HIGH (9.8)
- Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

References:
- OSSINDEX - [CVE-2016-1000027] CWE-502: Deserialization of Untrusted Data

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2020-5421 (OSSINDEX) suppress

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

CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:H/Au:/C:L/I:H/A:N

References:
- OSSINDEX - [CVE-2020-5421] CWE-noinfo

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2021-22096 (OSSINDEX) suppress

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

CWE-117 Improper Output Neutralization for Logs

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

References:
- OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2021-22118 (OSSINDEX) suppress

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

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

CWE-668 Exposure of Resource to Wrong Sphere

CVSSv2:
- Base Score: HIGH (7.8)
- Vector: /AV:L/AC:L/Au:/C:H/I:H/A:H

References:
- OSSINDEX - [CVE-2021-22118] CWE-668: Exposure of Resource to Wrong Sphere

Vulnerable Software & Versions (OSSINDEX):

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

spring-beans-5.2.3.RELEASE.jar

Description:

Spring Beans

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\spring-beans\5.2.3.RELEASE\spring-beans-5.2.3.RELEASE.jar
MD5: b64e8da412c3b6100f4bc0f54325d44f
SHA1: 0250c8c641433dc06b1b44e4563fa08a2fbf8954
SHA256:d3083070ad4eaf32e003b86ca0e7c0cb4fd2819800fef86ceb1043d387c14e2d
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-22965 (OSSINDEX) 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 (9.8)
- Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

References:
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')

Vulnerable Software & Versions (OSSINDEX):

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

spring-webmvc-5.2.3.RELEASE.jar

Description:

Spring Web MVC

License:

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

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

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2021-22060 (OSSINDEX) suppress

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

CWE-117 Improper Output Neutralization for Logs

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

References:
- OSSINDEX - [CVE-2021-22060] CWE-117: Improper Output Neutralization for Logs

Vulnerable Software & Versions (OSSINDEX):

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

spring-context-5.2.3.RELEASE.jar

Description:

Spring Context

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\spring-context\5.2.3.RELEASE\spring-context-5.2.3.RELEASE.jar
MD5: a5ba542a35f3c9fca630df1715ccf325
SHA1: 7750c95c96c7a1885c8b1b503ba915bc33ca579a
SHA256:82c625cffed80685b153700359a6c6d5c91018069a0171cf21a7defb0267e993
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-22968 (OSSINDEX) 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 (5.3)
- Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

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

Vulnerable Software & Versions (OSSINDEX):

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

spring-expression-5.2.3.RELEASE.jar

Description:

Spring Expression Language (SpEL)

License:

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

File Path: C:\Users\cacurtis\.m2\repository\org\springframework\spring-expression\5.2.3.RELEASE\spring-expression-5.2.3.RELEASE.jar
MD5: f2d2fe0e4f9b9b23b03d07839393de5a
SHA1: d0c6bb10758805b2153c589686b8045554bfac2d
SHA256:1ba798e1f4da9e5ad68e67d7e7abe39f141674762c8755d952edeb0380d384b9
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-22950 (OSSINDEX) 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 (6.5)
- Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:
- OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2023-20861 (OSSINDEX) suppress

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

CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:
- OSSINDEX - [CVE-2023-20861] CWE-noinfo

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2023-20863 (OSSINDEX) 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')

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:
- OSSINDEX - [CVE-2023-20863] CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

Vulnerable Software & Versions (OSSINDEX):

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

json-path-2.4.0.jar

Description:

Java port of Stefan Goessner JsonPath.

License:

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

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

Evidence

Identifiers

- pkg:maven/com.jayway.jsonpath/json-path@2.4.0 (*Confidence*:High)
- cpe:2.3:a:json-java_project:json-java:2.4.0:*:*:*:*:*:*:* (*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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://github.com/dromara/hutool/issues/2748
- MISC - 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: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://github.com/stleary/JSON-java/issues/758
- MISC - https://github.com/stleary/JSON-java/issues/771

Vulnerable Software & Versions:

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

json-smart-2.3.jar

Description:

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

License:

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

File Path: C:\Users\cacurtis\.m2\repository\net\minidev\json-smart\2.3\json-smart-2.3.jar
MD5: f2a921d4baaa7308de04eed4d8d72715
SHA1: 007396407491352ce4fa30de92efb158adb76b5b
SHA256:903f48c8aa4c3f6426440b8d32de89fa1dc23b1169abde25e4e1d068aa67708b
Referenced In Project/Scope:ssl-server:compile

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2021-27568 (OSSINDEX) suppress

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

CWE-754 Improper Check for Unusual or Exceptional Conditions

CVSSv2:
- Base Score: MEDIUM (5.9)
- Vector: /AV:N/AC:H/Au:/C:N/I:N/A:H

References:
- OSSINDEX - [CVE-2021-27568] CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2021-31684 (OSSINDEX) suppress

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

CWE-787 Out-of-bounds Write

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

References:
- OSSINDEX - [CVE-2021-31684] CWE-787: Out-of-bounds Write

Vulnerable Software & Versions (OSSINDEX):

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

CVE-2023-1370 (OSSINDEX) suppress

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

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

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

CWE-674 Uncontrolled Recursion

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

References:
- OSSINDEX - [CVE-2023-1370] CWE-674: Uncontrolled Recursion

Vulnerable Software & Versions (OSSINDEX):

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

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.