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

Sponsor

Project: engine

io.isotope.enigma:engine:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 8.0.2
- *Report Generated On*: Sun, 12 Feb 2023 19:32:56 +0100
- *Dependencies Scanned*: 116 (64 unique)
- *Vulnerable Dependencies*: 21
- *Vulnerabilities Found*: 137
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	C
bcprov-jdk15on-1.65.jar	cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.65:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.65:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.65:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.65:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.65	HIGH	3
hibernate-core-5.4.21.Final.jar	cpe:2.3:a:hibernate:hibernate_orm:5.4.21:*:*:*:*:*:*:*	pkg:maven/org.hibernate/hibernate-core@5.4.21.Final	HIGH	1
httpclient-4.5.12.jar	cpe:2.3:a:apache:httpclient:4.5.12:*:*:*:*:*:*:*	pkg:maven/org.apache.httpcomponents/httpclient@4.5.12	MEDIUM	1
jackson-databind-2.11.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.11.2:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.11.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.11.2	HIGH	3
jakarta.el-3.0.3.jar	cpe:2.3:a:eclipse:glassfish:3.0.3:*:*:*:*:*:*:* cpe:2.3:a:eclipse:jakarta_expression_language:3.0.3:*:*:*:*:*:*:*	pkg:maven/org.glassfish/jakarta.el@3.0.3	MEDIUM	1
keycloak-adapter-core-11.0.2.jar	cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:*	pkg:maven/org.keycloak/keycloak-adapter-core@11.0.2	CRITICAL	1
keycloak-core-11.0.2.jar	cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:*	pkg:maven/org.keycloak/keycloak-core@11.0.2	CRITICAL	2
liquibase-core-3.8.9.jar	cpe:2.3:a:liquibase:liquibase:3.8.9:*:*:*:*:*:*:*	pkg:maven/org.liquibase/liquibase-core@3.8.9	CRITICAL	1
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	MEDIUM	1
netty-transport-4.1.52.Final.jar	cpe:2.3:a:netty:netty:4.1.52:*:*:*:*:*:*:*	pkg:maven/io.netty/netty-transport@4.1.52.Final	HIGH	9
postgresql-42.2.16.jar	cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.2.16:*:*:*:*:*:*:*	pkg:maven/org.postgresql/postgresql@42.2.16	CRITICAL	4
reactor-netty-0.9.12.RELEASE.jar	cpe:2.3:a:pivotal:reactor_netty:0.9.12:release:*:*:*:*:*:*	pkg:maven/io.projectreactor.netty/reactor-netty@0.9.12.RELEASE	MEDIUM	1
snakeyaml-1.26.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.26:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.26	HIGH	7
spring-boot-2.3.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.3.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.3.4.RELEASE	HIGH	1
spring-boot-container-bundle-11.0.2.jar	cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:*	pkg:maven/org.keycloak/spring-boot-container-bundle@11.0.2	CRITICAL	1
spring-core-5.2.9.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.2.9.RELEASE	CRITICAL*	8
spring-security-core-5.3.4.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_security:5.3.4:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.3.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.security/spring-security-core@5.3.4.RELEASE	CRITICAL	4
spring-security-web-5.3.4.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_security:5.3.4:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.3.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.security/spring-security-web@5.3.4.RELEASE	CRITICAL	4

	cpe:2.3:a:web_project:web:5.3.4:release:*:*:*:*:*:*			
spring-web-5.2.9.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.9:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.9.RELEASE	CRITICAL*	9
spring-webmvc-5.2.9.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.9:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.2.9.RELEASE	CRITICAL*	8
tomcat-embed-core-9.0.38.jar	cpe:2.3:a:apache:tomcat:9.0.38:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.38:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.38	HIGH	1

* indicates the dependency has a known exploited vulnerability

Dependencies

bcprov-jdk15on-1.65.jar

Description:

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.8.

License:

Bouncy Castle Licence: http://www.bouncycastle.org/licence.html

File Path: /Users/djvelickovic/.m2/repository/org/bouncycastle/bcprov-jdk15on/1.65/bcprov-jdk15on-1.65.jar
MD5: 299b546652c9e1903685018342da0db0
SHA1: 320b989112f00a63a3bcfa5a98f31a4f865a20fa
SHA256:e78f96eb59066c94c94fb2d6b5eb80f52feac6f5f9776898634f8addec6e2137
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.keycloak/keycloak-spring-boot-starter@11.0.2

Evidence

Identifiers

- pkg:maven/org.bouncycastle/bcprov-jdk15on@1.65 (*Confidence*:High)
- cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.65:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.65:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.65:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.65:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2020-28052 suppress

An issue was discovered in Legion of the Bouncy Castle BC Java 1.65 and 1.66. The OpenBSDBCrypt.checkPassword utility method compared incorrect data when checking the password, allowing incorrect passwords to indicate they were matching with previously hashed ones that were different.

NVD-CWE-Other

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

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://github.com/bcgit/bc-java/wiki/CVE-2020-28052
- MISC - https://www.bouncycastle.org/releasenotes.html
- 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
- MISC - https://www.synopsys.com/blogs/software-security/cve-2020-28052-bouncy-castle/
- MLIST - [druid-commits] 20210107 [GitHub] [druid] clintropolis merged pull request #10733: Update deps for CVE-2020-28168 and CVE-2020-28052
- MLIST - [druid-commits] 20210107 [GitHub] [druid] jon-wei opened a new pull request #10733: Update deps for CVE-2020-28168 and CVE-2020-28052
- MLIST - [druid-commits] 20210127 [druid] 01/02: Update deps for CVE-2020-28168 and CVE-2020-28052 (#10733)
- MLIST - [kafka-jira] 20210107 [GitHub] [kafka] cyrusv opened a new pull request #9845: MINOR: Bump Bouncy Castle Dep to resolve CVE-2020-28052
- MLIST - [karaf-issues] 20210810 [jira] [Commented] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210810 [jira] [Created] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210810 [jira] [Updated] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210816 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.69 artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210816 [jira] [Updated] (KARAF-7240) Upgrade bcprov artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210817 [jira] [Commented] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210817 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210820 [jira] [Updated] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210824 [jira] [Commented] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
- MLIST - [karaf-issues] 20210824 [jira] [Resolved] (KARAF-7240) Upgrade bcprov 1.68 artifacts to mitigate CVE-2020-28052
- MLIST - [pulsar-commits] 20210119 [GitHub] [pulsar] fmiguelez opened a new issue #9235: Upgrade Bounce Castle dependency on client to solve CVE-2020-

28052
- MLIST - [pulsar-commits] 20210406 [GitHub] [pulsar] lhotari commented on issue #9235: Upgrade Bounce Castle dependency on client to solve CVE-2020-28052
- MLIST - [solr-issues] 20210525 [jira] [Created] (SOLR-15431) Security vulnerability with Bouncy Castle library within Apache Solr 8.8.2
- N/A - N/A
- N/A - N/A
- OSSINDEX - [CVE-2020-28052] CWE-Other
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-28052
- OSSIndex - https://www.synopsys.com/blogs/software-security/cve-2020-28052-bouncy-castle/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.65:*:*:*:*:*:*:*
- ...

CVE-2020-15522 suppress

Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.

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

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

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210622-0007/
- MISC - https://github.com/bcgit/bc-csharp/wiki/CVE-2020-15522
- MISC - https://github.com/bcgit/bc-java/wiki/CVE-2020-15522
- MISC - https://www.bouncycastle.org/releasenotes.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:*:*:*:*:*:*:*:* versions up to (excluding) 1.66
- ...

CVE-2020-0187 (OSSINDEX) suppress

In engineSetMode of BaseBlockCipher.java, there is a possible incorrect cryptographic algorithm chosen due to an incomplete comparison. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148517383

CWE-310 Cryptographic Issues

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:L/AC:L/Au:/C:H/I:N/A:N

References:
- OSSINDEX - [CVE-2020-0187] CWE-310
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0187
- OSSIndex - https://android.googlesource.com/platform/external/bouncycastle/+/14ceec126e49f2f4748f0d540be820515cc725a6
- OSSIndex - https://source.android.com/security/bulletin/pixel/2020-06-01

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.65:*:*:*:*:*:*:*

hibernate-core-5.4.21.Final.jar

Description:

Hibernate's core ORM functionality

License:

GNU Library General Public License v2.1 or later: http://www.opensource.org/licenses/LGPL-2.1

File Path: /Users/djvelickovic/.m2/repository/org/hibernate/hibernate-core/5.4.21.Final/hibernate-core-5.4.21.Final.jar
MD5: ffccd758877152a6b59d970ab138cc91
SHA1: 7cc737047ce084bf732adbb7f4064a16fd26229a
SHA256:568b6212aacbc04b57b1ea55a193e9d09ba2f8802286a64270d71baa782d9ddc
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-data-jpa@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.hibernate/hibernate-core@5.4.21.Final (*Confidence*:High)
- cpe:2.3:a:hibernate:hibernate_orm:5.4.21:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2020-25638 suppress

A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.

CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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

CVSSv3:
- Base Score: HIGH (7.4)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

References:
- DEBIAN - DSA-4908
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1881353
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MLIST - [debian-lts-announce] 20210103 [SECURITY] [DLA 2512-1] libhibernate3-java security update
- MLIST - [turbine-commits] 20211018 [turbine-fulcrum-security] 02/02: disable module hibernate (JIRA issue TRB-103), update docs, remove suppression
- MLIST - [turbine-dev] 20211015 Fulcrum Security Hibernate Module
- N/A - N/A
- N/A - N/A
- OSSINDEX - [CVE-2020-25638] CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25638
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=1881353
- OSSIndex - https://hibernate.atlassian.net/browse/HHH-14225

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:hibernate:hibernate_orm:*:*:*:*:*:*:*:* versions from (including) 5.4.0; versions up to (excluding) 5.4.24
- ...

httpclient-4.5.12.jar

Description:

Apache HttpComponents Client

File Path: /Users/djvelickovic/.m2/repository/org/apache/httpcomponents/httpclient/4.5.12/httpclient-4.5.12.jar
MD5: 72002652711fe0fa3218d2bf20f47409
SHA1: 4023a2a80b64c25926911faf350b50cd2a29220f
SHA256:bc5f065aba5dd815ee559dd24d9bcb797fb102ff9cfa036f5091ebc529bd3b93
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.keycloak/keycloak-spring-boot-starter@11.0.2

Evidence

Identifiers

- pkg:maven/org.apache.httpcomponents/httpclient@4.5.12 (*Confidence*:High)
- cpe:2.3:a:apache:httpclient:4.5.12:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-13956 suppress

Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution.

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220210-0002/
- MISC - https://lists.apache.org/thread.html/r6dab7da30f8bf075f79ee189e33b45a197502e2676481bb8787fc0d7%40%3Cdev.hc.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
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html

- MLIST - [bookkeeper-issues] 20210914 [GitHub] [bookkeeper] nicoloboschi opened a new pull request #2793: Upgrade httpclient from 4.5.5 to 4.5.13 to address CVE-2020-13956
- MLIST - [bookkeeper-issues] 20210917 [GitHub] [bookkeeper] nicoloboschi commented on pull request #2793: Upgrade httpclient from 4.5.5 to 4.5.13 to address CVE-2020-13956
- MLIST - [creadur-commits] 20210608 [jira] [Assigned] (TENTACLES-13) Upgrade httpclient to circumvent CVE-2020-13956
- MLIST - [creadur-commits] 20210608 [jira] [Commented] (TENTACLES-13) Upgrade httpclient to circumvent CVE-2020-13956
- MLIST - [creadur-commits] 20210608 [jira] [Created] (TENTACLES-13) Upgrade httpclient to circumvent CVE-2020-13956
- MLIST - [creadur-commits] 20210608 [jira] [Resolved] (TENTACLES-13) Upgrade httpclient to circumvent CVE-2020-13956
- MLIST - [creadur-commits] 20210608 [jira] [Work started] (TENTACLES-13) Upgrade httpclient to circumvent CVE-2020-13956
- MLIST - [creadur-dev] 20210621 [jira] [Updated] (RAT-275) Update httpclient to fix CVE-2020-13956 once a new doxia-core release is available
- MLIST - [drill-commits] 20210604 [drill] branch master updated: DRILL-7946: Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956 (#2250)
- MLIST - [drill-dev] 20210604 [GitHub] [drill] cgivre commented on pull request #2250: DRILL-7946: Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-dev] 20210604 [GitHub] [drill] laurentgo merged pull request #2250: DRILL-7946: Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-dev] 20210604 [GitHub] [drill] luocooong commented on pull request #2250: DRILL-7946: Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-dev] 20210604 [GitHub] [drill] luocooong opened a new pull request #2250: DRILL-7946: Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-dev] 20210604 [jira] [Created] (DRILL-7946) Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-dev] 20210604 [jira] [Resolved] (DRILL-7946) Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-issues] 20210604 [jira] [Commented] (DRILL-7946) Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-issues] 20210604 [jira] [Created] (DRILL-7946) Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [drill-issues] 20210604 [jira] [Resolved] (DRILL-7946) Bump HttpClient from 4.5.12 to 4.5.13 for CVE-2020-13956
- MLIST - [hive-dev] 20210301 [jira] [Created] (HIVE-24837) Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [hive-gitbox] 20210301 [GitHub] [hive] hsnusonic opened a new pull request #2032: HIVE-24837 Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [hive-gitbox] 20210302 [GitHub] [hive] hsnusonic closed pull request #2032: HIVE-24837 Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [hive-issues] 20210301 [jira] [Assigned] (HIVE-24837) Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [hive-issues] 20210301 [jira] [Updated] (HIVE-24837) Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [hive-issues] 20210301 [jira] [Work logged] (HIVE-24837) Upgrade httpclient to 4.5.13+ due to CVE-2020-13956
- MLIST - [jackrabbit-dev] 20210706 [GitHub] [jackrabbit-oak] reschke commented on pull request #310: OAK-9482: upgrade httpclient to 4.5.13
- MLIST - [jackrabbit-dev] 20210706 [GitHub] [jackrabbit-oak] reschke removed a comment on pull request #310: OAK-9482: upgrade httpclient to 4.5.13
- MLIST - [lucene-issues] 20210921 [GitHub] [lucene-solr] madrob commented on pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20210921 [GitHub] [lucene-solr] ventry1990 commented on pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20210921 [GitHub] [lucene-solr] ventry1990 opened a new pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20211007 [GitHub] [lucene-solr] madrob commented on pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20211009 [GitHub] [lucene-solr] ventry1990 closed pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20211009 [GitHub] [lucene-solr] ventry1990 commented on pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20211009 [GitHub] [lucene-solr] ventry1990 opened a new pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-issues] 20211011 [GitHub] [lucene-solr] madrob merged pull request #2579: SOLR-15269: Upgrade Apache HttpComponents Client to 4.5.13 to fix CVE-2020-13956
- MLIST - [lucene-solr-user] 20201229 Upgrade httpclient version due to CVE-2020-13956?
- MLIST - [maven-issues] 20210530 [jira] [Closed] (DOXIA-615) Can you provide an updated version in order to fix CVE-2020-13956
- MLIST - [maven-issues] 20210530 [jira] [Resolved] (DOXIA-615) Can you provide an updated version in order to fix CVE-2020-13956
- MLIST - [maven-issues] 20210530 [jira] [Updated] (DOXIA-615) Can you provide an updated version in order to fix CVE-2020-13956
- MLIST - [maven-issues] 20210621 [jira] [Assigned] (DOXIA-615) Can you provide an updated version in order to fix CVE-2020-13956
- MLIST - [pulsar-commits] 20201215 [GitHub] [pulsar] yanshuchong opened a new issue #8967: CVSS issue list
- MLIST - [ranger-dev] 20201204 [jira] [Assigned] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [ranger-dev] 20201204 [jira] [Updated] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [ranger-dev] 20201215 [jira] [Commented] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [ranger-dev] 20201215 [jira] [Updated] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [ranger-dev] 20201216 [jira] [Commented] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [ranger-dev] 20211028 [jira] [Commented] (RANGER-3100) Upgrade httpclient version from 4.5.6 to 4.5.13+ due to CVE-2020-13956
- MLIST - [solr-issues] 20210316 [jira] [Created] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20210316 [jira] [Created] (SOLR-15270) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20210316 [jira] [Resolved] (SOLR-15270) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20210623 [jira] [Updated] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20210623 [jira] [Updated] (SOLR-15270) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20210912 [jira] [Updated] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20211011 [jira] [Commented] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20211011 [jira] [Resolved] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [solr-issues] 20211019 [jira] [Closed] (SOLR-15269) upgrade httpclient to address CVE-2020-13956
- MLIST - [turbine-commits] 20210203 svn commit: r1886168 - in /turbine/core/trunk: ./ conf/ conf/test/ src/java/org/apache/turbine/services/urlmapper/ src/test/org/apache/turbine/services/urlmapper/ src/test/org/apache/turbine/services/urlmapper/model/ xdocs/howto/
- N/A - N/A
- OSSINDEX - [CVE-2020-13956] CWE-20: Improper Input Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13956
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=1886587
- OSSIndex - https://www.openwall.com/lists/oss-security/2020/10/08/4

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:httpclient:*:*:*:*:*:*:*:* versions up to (excluding) 4.5.13
- ...

jackson-databind-2.11.2.jar

Description:

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

License:

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

File Path: /Users/djvelickovic/.m2/repository/com/fasterxml/jackson/core/jackson-databind/2.11.2/jackson-databind-2.11.2.jar
MD5: 14fd0effa4d1d3e09edb36423be82aff
SHA1: ee08bbd8975dde844307fe8309dfcd5ec7ee129d

SHA256:cb890b4aad8ed21a7b57e3c8f7924dbdca1aeff9ddd27cb0ff37243037ae1342
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.11.2 (*Confidence*:High)
- cpe:2.3:a:fasterxml:jackson-databind:2.11.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:fasterxml:jackson-modules-java8:2.11.2:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2020-36518 suppress

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

CWE-787 Out-of-bounds Write

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

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

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/2816

Vulnerable Software & Versions: (show all)

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

CVE-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: CVSS:3.1/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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42003
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=51020
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3590

Vulnerable Software & Versions: (show all)

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

CVE-2022-42004 suppress

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

CWE-502 Deserialization of Untrusted Data

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

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42004
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/3582

Vulnerable Software & Versions: (show all)

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

jakarta.el-3.0.3.jar

Description:

Jakarta Expression Language provides a specification document, API, reference implementation and TCK that describes an expression language for Java applications.

License:

EPL 2.0: http://www.eclipse.org/legal/epl-2.0
GPL2 w/ CPE: https://www.gnu.org/software/classpath/license.html

File Path: /Users/djvelickovic/.m2/repository/org/glassfish/jakarta.el/3.0.3/jakarta.el-3.0.3.jar
MD5: 6bb54dbf912bf1b6c79592838db76b51
SHA1: dab46ee1ee23f7197c13d7c40fce14817c9017df
SHA256:e2bcb8551b02a5c2afdc4cab77302ba5c76705cf1fc832345ca880df80bf4716
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.glassfish/jakarta.el@3.0.3 (*Confidence*:High)
- cpe:2.3:a:eclipse:glassfish:3.0.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:eclipse:jakarta_expression_language:3.0.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2021-28170 suppress

In the Jakarta Expression Language implementation 3.0.3 and earlier, a bug in the ELParserTokenManager enables invalid EL expressions to be evaluated as if they were valid.

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

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://github.com/eclipse-ee4j/el-ri/issues/155
- CONFIRM - https://securitylab.github.com/advisories/GHSL-2020-021-jakarta-el/
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:eclipse:jakarta_expression_language:*:*:*:*:*:*:*:* versions up to (including) 3.0.3
- ...

keycloak-adapter-core-11.0.2.jar

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/keycloak/keycloak-adapter-core/11.0.2/keycloak-adapter-core-11.0.2.jar
MD5: 1ea0186a8809712dba12a648ac6aad0d
SHA1: 28ea7a5662fa5f21f9e969ff093fb7656966b1d4
SHA256:c7efc25ece7a84c8712cbed824b9819aa4b335f9efc82563bc4cfd439aa40f75

Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.keycloak/keycloak-spring-boot-starter@11.0.2

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.keycloak/keycloak-adapter-core@11.0.2 (*Confidence*:High)
- cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-1245 suppress

A privilege escalation flaw was found in the token exchange feature of keycloak. Missing authorization allows a client application holding a valid access token to exchange tokens for any target client by passing the client_id of the target. This could allow a client to gain unauthorized access to additional services.

CWE-862 Missing Authorization

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

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

References:
- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-75p6-52g3-rqc8

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0

CVE-2021-20195 suppress

A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CWE-116 Improper Encoding or Escaping of Output

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

CVSSv3:
- Base Score: CRITICAL (9.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1919143

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.3

CVE-2020-14389 suppress

It was found that Keycloak before version 12.0.0 would permit a user with only view-profile role to manage the resources in the new account console, allowing access and modification of data the user was not intended to have.

CWE-916 Use of Password Hash With Insufficient Computational Effort

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- MISC - https://access.redhat.com/security/cve/cve-2020-14389
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1875843,

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2020-14366 suppress

A vulnerability was found in keycloak, where path traversal using URL-encoded path segments in the request is possible because the resources endpoint applies a transformation of the url path to the file path. Only few specific folder hierarchies can be exposed by this flaw

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

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

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

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14366

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-20222 suppress

A flaw was found in keycloak. The new account console in keycloak can allow malicious code to be executed using the referrer URL. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

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

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1924606

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 13.0.0

CVE-2021-3513 suppress

A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enabled. This is due to a wrong error message displayed when wrong credentials are entered. The highest threat from this vulnerability is to confidentiality.

CWE-209 Information Exposure Through an Error Message

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3513
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1953439

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3632 suppress

A flaw was found in Keycloak. This vulnerability allows anyone to register a new security device or key when there is not a device already registered for any user by using the WebAuthn password-less login flow.

CWE-287 Improper Authentication

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3632
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1978196
- MISC - https://github.com/keycloak/keycloak/commit/65480cb5a11630909c086f79d396004499fbd1e4
- MISC - https://github.com/keycloak/keycloak/pull/8203
- MISC - https://issues.redhat.com/browse/KEYCLOAK-18500

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0
- ...

CVE-2021-3637 suppress

A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1979638

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 14.0.0
- ...

CVE-2021-20202 suppress

A flaw was found in keycloak. Directories can be created prior to the Java process creating them in the temporary directory, but with wider user permissions, allowing the attacker to have access to the contents that keycloak stores in this directory. The highest threat from this vulnerability is to data confidentiality and integrity.

CWE-377 Insecure Temporary File

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

CVSSv3:
- Base Score: HIGH (7.3)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1922128

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3827 suppress

A flaw was found in keycloak, where the default ECP binding flow allows other authentication flows to be bypassed. By exploiting this behavior, an attacker can bypass the MFA authentication by sending a SOAP request with an AuthnRequest and Authorization header with the user's credentials. The highest threat from this vulnerability is to confidentiality and integrity.

CWE-287 Improper Authentication

CVSSv3:
- Base Score: MEDIUM (6.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3827
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2007512
- MISC - https://github.com/keycloak/keycloak/commit/44000caaf5051d7f218d1ad79573bd3d175cad0d
- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-4pc7-vqv5-5r3v

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0
- ...

CVE-2020-27838 suppress

A flaw was found in keycloak in versions prior to 13.0.0. The client registration endpoint allows fetching information about PUBLIC clients (like client secret) without authentication which could be an issue if the same PUBLIC client changed to CONFIDENTIAL later. The highest threat from this vulnerability is to data confidentiality.

CWE-287 Improper Authentication

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1906797

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0
- ...

CVE-2022-1466 suppress

Due to improper authorization, Red Hat Single Sign-On is vulnerable to users performing actions that they should not be allowed to perform. It was possible to add users to the master realm even though no respective permission was granted.

CWE-863 Incorrect Authorization

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2050228
- MISC - https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-076.txt
- MISC - https://www.syss.de/pentest-blog/fehlerhafte-autorisierung-bei-red-hat-single-sign-on-750ga-syss-2021-076

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.1
- ...

CVE-2021-20323 suppress

A POST based reflected Cross Site Scripting vulnerability on has been identified in Keycloak.

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

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2013577

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.0

CVE-2020-1725 suppress

A flaw was found in keycloak before version 13.0.0. In some scenarios a user still has access to a resource after changing the role mappings in Keycloak and after expiration of the previous access token.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1765129
- MISC - https://issues.redhat.com/browse/KEYCLOAK-16550

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10770 suppress

A flaw was found in Keycloak before 13.0.0, where it is possible to force the server to call out an unverified URL using the OIDC parameter request_uri. This flaw allows an attacker to use this parameter to execute a Server-side request forgery (SSRF) attack.

CWE-918 Server-Side Request Forgery (SSRF)

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - http://packetstormsecurity.com/files/164499/Keycloak-12.0.1-Server-Side-Request-Forgery.html
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1846270

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.2

CVE-2020-14302 suppress

A flaw was found in Keycloak before 13.0.0 where an external identity provider, after successful authentication, redirects to a Keycloak endpoint that accepts multiple invocations with the use of the same "state" parameter. This flaw allows a malicious user to perform replay attacks.

CWE-294 Authentication Bypass by Capture-replay

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

CVSSv3:
- Base Score: MEDIUM (4.9)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1849584

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10776 suppress

A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack.

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

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

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1847428

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-3856 suppress

ClassLoaderTheme and ClasspathThemeResourceProviderFactory allows reading any file available as a resource to the classloader. By sending requests for theme resources with a relative path from an external HTTP client, the client will receive the content of random files if available.

CWE-552 Files or Directories Accessible to External Parties

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3856
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2010164
- MISC - https://github.com/keycloak/keycloak/commit/73f0474008e1bebd0733e62a22aceda9e5de6743
- MISC - https://github.com/keycloak/keycloak/pull/8588
- MISC - https://issues.redhat.com/browse/KEYCLOAK-19422

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0

CVE-2020-27826 suppress

A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker to change its own NameID attribute to impersonate the admin user for any particular application.

CWE-250 Execution with Unnecessary Privileges

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.2)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1905089

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0
- ...

keycloak-core-11.0.2.jar

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/keycloak/keycloak-core/11.0.2/keycloak-core-11.0.2.jar
MD5: 5ec016ff8dc6e327bd0b10670d094216
SHA1: be62ed42a57a1aa616325780362bedd377595841
SHA256:ae74a7d805977973100ede4107c1d9674efbbeaadca4b3e9b1d19790183b2f23
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.keycloak/keycloak-spring-boot-starter@11.0.2

Evidence

Identifiers

- pkg:maven/org.keycloak/keycloak-core@11.0.2 (*Confidence*:High)
- cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-1245 suppress

A privilege escalation flaw was found in the token exchange feature of keycloak. Missing authorization allows a client application holding a valid access token to exchange tokens for any target client by passing the client_id of the target. This could allow a client to gain unauthorized access to additional services.

CWE-862 Missing Authorization

CVSSv2:
- Base Score: HIGH (7.5)

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

CVSSv3:

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

References:

- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-75p6-52g3-rqc8

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0

CVE-2021-20195 suppress

A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CWE-116 Improper Encoding or Escaping of Output

CVSSv2:

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

CVSSv3:

- Base Score: CRITICAL (9.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:

- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1919143

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.3

CVE-2020-14389 suppress

It was found that Keycloak before version 12.0.0 would permit a user with only view-profile role to manage the resources in the new account console, allowing access and modification of data the user was not intended to have.

CWE-916 Use of Password Hash With Insufficient Computational Effort

CVSSv2:

- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:

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

References:

- MISC - https://access.redhat.com/security/cve/cve-2020-14389
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1875843,

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2020-14366 suppress

A vulnerability was found in keycloak, where path traversal using URL-encoded path segments in the request is possible because the resources endpoint applies a transformation of the url path to the file path. Only few specific folder hierarchies can be exposed by this flaw

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

CVSSv2:

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

CVSSv3:

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

References:

- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14366

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-20222 suppress

A flaw was found in keycloak. The new account console in keycloak can allow malicious code to be executed using the referrer URL. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

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

CVSSv2:

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

CVSSv3:

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

References:

- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1924606

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 13.0.0

CVE-2021-3513 suppress

A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enabled. This is due to a wrong error message displayed when wrong credentials are entered. The highest threat from this vulnerability is to confidentiality.

CWE-209 Information Exposure Through an Error Message

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3513
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1953439

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3632 suppress

A flaw was found in Keycloak. This vulnerability allows anyone to register a new security device or key when there is not a device already registered for any user by using the WebAuthn password-less login flow.

CWE-287 Improper Authentication

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3632
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1978196
- MISC - https://github.com/keycloak/keycloak/commit/65480cb5a11630909c086f79d396004499fbd1e4
- MISC - https://github.com/keycloak/keycloak/pull/8203
- MISC - https://issues.redhat.com/browse/KEYCLOAK-18500

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0
- ...

CVE-2021-3637 suppress

A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1979638

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 14.0.0
- ...

CVE-2021-20202 suppress

A flaw was found in keycloak. Directories can be created prior to the Java process creating them in the temporary directory, but with wider user permissions, allowing the attacker to have access to the contents that keycloak stores in this directory. The highest threat from this vulnerability is to data confidentiality and integrity.

CWE-377 Insecure Temporary File

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

CVSSv3:
- Base Score: HIGH (7.3)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1922128

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3827 suppress

A flaw was found in keycloak, where the default ECP binding flow allows other authentication flows to be bypassed. By exploiting this behavior, an attacker can bypass the MFA authentication by sending a SOAP request with an AuthnRequest and Authorization header with the user's credentials. The highest threat from this vulnerability is to confidentiality and integrity.

CWE-287 Improper Authentication

CVSSv3:

- Base Score: MEDIUM (6.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3827
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2007512
- MISC - https://github.com/keycloak/keycloak/commit/44000caaf5051d7f218d1ad79573bd3d175cad0d
- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-4pc7-vqv5-5r3v

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0
- ...

CVE-2020-27838 suppress

A flaw was found in keycloak in versions prior to 13.0.0. The client registration endpoint allows fetching information about PUBLIC clients (like client secret) without authentication which could be an issue if the same PUBLIC client changed to CONFIDENTIAL later. The highest threat from this vulnerability is to data confidentiality.

CWE-287 Improper Authentication

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1906797

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0
- ...

CVE-2022-1466 suppress

Due to improper authorization, Red Hat Single Sign-On is vulnerable to users performing actions that they should not be allowed to perform. It was possible to add users to the master realm even though no respective permission was granted.

CWE-863 Incorrect Authorization

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2050228
- MISC - https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-076.txt
- MISC - https://www.syss.de/pentest-blog/fehlerhafte-autorisierung-bei-red-hat-single-sign-on-750ga-syss-2021-076
- OSSINDEX - [CVE-2022-1466] CWE-863: Incorrect Authorization
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1466
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=2050228
- OSSIndex - https://github.com/advisories/GHSA-f32v-vf79-p29g
- OSSIndex - https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-076.txt

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.1
- ...

CVE-2023-0105 (OSSINDEX) suppress

A flaw was found in Keycloak. This flaw allows impersonation and lockout due to the email trust not being handled correctly in Keycloak. An attacker can shadow other users with the same email and lockout or impersonate them.

CWE-287 Improper Authentication

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

References:
- OSSINDEX - [CVE-2023-0105] CWE-287: Improper Authentication
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-0105
- OSSIndex - https://github.com/advisories/GHSA-vhvq-jh34-3fc8

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.keycloak:keycloak-core:11.0.2:*:*:*:*:*:*:*

CVE-2021-20323 suppress

A POST based reflected Cross Site Scripting vulnerability on has been identified in Keycloak.

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

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

CVSSv3:
- Base Score: MEDIUM (6.1)

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2013577

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.0

CVE-2020-1725 suppress

A flaw was found in keycloak before version 13.0.0. In some scenarios a user still has access to a resource after changing the role mappings in Keycloak and after expiration of the previous access token.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1765129
- MISC - https://issues.redhat.com/browse/KEYCLOAK-16550

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10770 suppress

A flaw was found in Keycloak before 13.0.0, where it is possible to force the server to call out an unverified URL using the OIDC parameter request_uri. This flaw allows an attacker to use this parameter to execute a Server-side request forgery (SSRF) attack.

CWE-918 Server-Side Request Forgery (SSRF)

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - http://packetstormsecurity.com/files/164499/Keycloak-12.0.1-Server-Side-Request-Forgery.html
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1846270

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.2

CVE-2020-14302 suppress

A flaw was found in Keycloak before 13.0.0 where an external identity provider, after successful authentication, redirects to a Keycloak endpoint that accepts multiple invocations with the use of the same "state" parameter. This flaw allows a malicious user to perform replay attacks.

CWE-294 Authentication Bypass by Capture-replay

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

CVSSv3:
- Base Score: MEDIUM (4.9)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1849584

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10776 suppress

A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack.

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

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

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1847428

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-3856 suppress

ClassLoaderTheme and ClasspathThemeResourceProviderFactory allows reading any file available as a resource to the classloader. By sending requests for theme resources with a relative path from an external HTTP client, the client will receive the content of random files if available.

CWE-552 Files or Directories Accessible to External Parties

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3856
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2010164
- MISC - https://github.com/keycloak/keycloak/commit/73f0474008e1bebd0733e62a22aceda9e5de6743
- MISC - https://github.com/keycloak/keycloak/pull/8588
- MISC - https://issues.redhat.com/browse/KEYCLOAK-19422

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0

CVE-2020-27826 suppress

A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker to change its own NameID attribute to impersonate the admin user for any particular application.

CWE-250 Execution with Unnecessary Privileges

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.2)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1905089

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0
- ...

liquibase-core-3.8.9.jar

Description:

Liquibase is a tool for managing and executing database changes.

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/liquibase/liquibase-core/3.8.9/liquibase-core-3.8.9.jar
MD5: 36826e30e0d0d109a745c0a7ea6c336a
SHA1: ba38ad9bc271fb4f5c03547f99ab22caecf70431
SHA256:ef6793c98c589d70baa56da1ea0138f3d14d7e8c8fa8751ed926ddfd296b3b39
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/io.isotope.enigma/engine@0.0.1-SNAPSHOT

Evidence

Identifiers

- pkg:maven/org.liquibase/liquibase-core@3.8.9 (*Confidence*:High)
- cpe:2.3:a:liquibase:liquibase:3.8.9:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-0839 suppress

Improper Restriction of XML External Entity Reference in GitHub repository liquibase/liquibase prior to 4.8.0.

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

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

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

References:
- CONFIRM - https://huntr.dev/bounties/f1ae5779-b406-4594-a8a3-d089c68d6e70
- MISC - https://github.com/liquibase/liquibase/commit/33d9d925082097fb1a3d2fc8e44423d964cd9381
- N/A - N/A
- OSSINDEX - [CVE-2022-0839] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0839
- OSSIndex - https://github.com/liquibase/liquibase/pull/2384
- OSSIndex - https://huntr.dev/bounties/f1ae5779-b406-4594-a8a3-d089c68d6e70/

Vulnerable Software & Versions:

- cpe:2.3:a:liquibase:liquibase:*:*:*:*:*:*:*:* versions up to (excluding) 4.8.0

logback-core-1.2.3.jar

Description:

logback-core module

License:

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

File Path: /Users/djvelickovic/.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: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

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: CVSS:3.1/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 - [sonatype-2021-4517] CWE-502: Deserialization of Untrusted Data
- OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591

Vulnerable Software & Versions: (show all)

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

netty-transport-4.1.52.Final.jar

Description:

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers and clients.

License:

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

File Path: /Users/djvelickovic/.m2/repository/io/netty/netty-transport/4.1.52.Final/netty-transport-4.1.52.Final.jar
MD5: 973eef4e4ca3ef4538b22c23efecff80
SHA1: 970ee3790f504452bd32692f6b208a590c51f0ee
SHA256:9a3e6f8c0e55de363eb1ea10fe781797eca394e62186df2ae0b4eb2bce0b4541
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-webflux@2.3.4.RELEASE

Evidence

Related Dependencies

Identifiers

- pkg:maven/io.netty/netty-transport@4.1.52.Final (*Confidence*:High)
- cpe:2.3:a:netty:netty:4.1.52:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2021-37136 suppress

The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220210-0012/
- DEBIAN - DSA-5316
- MISC - https://github.com/netty/netty/security/advisories/GHSA-grg4-wf29-r9vv
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [debian-lts-announce] 20230111 [SECURITY] [DLA 3268-1] netty security update
- MLIST - [druid-commits] 20211025 [GitHub] [druid] a2l007 commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211025 [GitHub] [druid] jihoonson commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211025 [GitHub] [druid] jihoonson opened a new pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211026 [GitHub] [druid] clintropolis merged pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211026 [GitHub] [druid] jihoonson commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [tinkerpop-dev] 20211025 [jira] [Created] (TINKERPOP-2632) Netty 4.1.61 flagged with two high severity security violations
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.68
- ...

CVE-2021-37137 suppress

The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer reserved skippable chunks until the whole chunk was received which may lead to excessive memory usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk.

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220210-0012/
- DEBIAN - DSA-5316
- MISC - https://github.com/netty/netty/security/advisories/GHSA-9vjp-v76f-g363
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [debian-lts-announce] 20230111 [SECURITY] [DLA 3268-1] netty security update
- MLIST - [druid-commits] 20211025 [GitHub] [druid] a2l007 commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3

- MLIST - [druid-commits] 20211025 [GitHub] [druid] jihoonson commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211025 [GitHub] [druid] jihoonson opened a new pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211026 [GitHub] [druid] clintropolis merged pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [druid-commits] 20211026 [GitHub] [druid] jihoonson commented on pull request #11844: Bump netty4 to 4.1.68; suppress CVE-2021-37136 and CVE-2021-37137 for netty3
- MLIST - [tinkerpop-dev] 20211025 [jira] [Created] (TINKERPOP-2632) Netty 4.1.61 flagged with two high severity security violations
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.68
- ...

CVE-2022-41881 suppress

Netty project is an event-driven asynchronous network application framework. In versions prior to 4.1.86.Final, a StackOverflowError can be raised when parsing a malformed crafted message due to an infinite recursion. This issue is patched in version 4.1.86.Final. There is no workaround, except using a custom HaProxyMessageDecoder.

CWE-674 Uncontrolled Recursion

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20230113-0004/
- DEBIAN - DSA-5316
- MISC - https://github.com/netty/netty/security/advisories/GHSA-fx2c-96vj-985v
- MLIST - [debian-lts-announce] 20230111 [SECURITY] [DLA 3268-1] netty security update

Vulnerable Software & Versions:

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.86

CVE-2021-43797 suppress

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. Netty prior to version 4.1.71.Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.71.Final.

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

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://github.com/netty/netty/security/advisories/GHSA-wx5j-54mm-rqqq
- CONFIRM - https://security.netapp.com/advisory/ntap-20220107-0003/
- DEBIAN - DSA-5316
- MISC - https://github.com/netty/netty/commit/07aa6b5938a8b6ed7a6586e066400e2643897323
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MLIST - [debian-lts-announce] 20230111 [SECURITY] [DLA 3268-1] netty security update
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.71
- ...

CVE-2022-41915 suppress

Netty project is an event-driven asynchronous network application framework. Starting in version 4.1.83.Final and prior to 4.1.86.Final, when calling `DefaultHttpHeadesr.set` with an _iterator_ of values, header value validation was not performed, allowing malicious header values in the iterator to perform HTTP Response Splitting. This issue has been patched in version 4.1.86.Final. Integrators can work around the issue by changing the `DefaultHttpHeaders.set(CharSequence, Iterator<?>)` call, into a `remove()` call, and call `add()` in a loop over the iterator of values.

CWE-436 Interpretation Conflict, CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20230113-0004/
- DEBIAN - DSA-5316
- MISC - https://github.com/netty/netty/commit/fe18adff1c2b333acb135ab779a3b9ba3295a1c4
- MISC - https://github.com/netty/netty/issues/13084
- MISC - https://github.com/netty/netty/pull/12760
- MISC - https://github.com/netty/netty/security/advisories/GHSA-hh82-3pmq-7frp
- MLIST - [debian-lts-announce] 20230111 [SECURITY] [DLA 3268-1] netty security update

Vulnerable Software & Versions:

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.86

CVE-2021-21295 suppress

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.60.Final there is a vulnerability that enables request smuggling. If a Content-Length header is present in the original HTTP/2 request, the field is not validated by `Http2MultiplexHandler` as it is propagated up. This is fine as long as the request is not proxied through as HTTP/1.1. If the request comes in as an HTTP/2 stream, gets converted into the HTTP/1.1 domain objects (`HttpRequest`, `HttpContent`, etc.) via `Http2StreamFrameToHttpObjectCodec `and then sent up to the child channel's pipeline and proxied through a remote peer as HTTP/1.1 this may result in request smuggling. In a proxy case, users may assume the content-length is validated somehow, which is not the case. If the request is forwarded to a backend channel that is a HTTP/1.1 connection, the Content-Length now has meaning and needs to be checked. An attacker can smuggle requests inside the body as it gets downgraded from HTTP/2 to HTTP/1.1. For an example attack refer to the linked GitHub Advisory. Users are only affected if all of this is true: `HTTP2MultiplexCodec` or `Http2FrameCodec` is used, `Http2StreamFrameToHttpObjectCodec` is used to convert to HTTP/1.1 objects, and these HTTP/1.1 objects are forwarded to another remote peer. This has been patched in 4.1.60.Final As a workaround, the user can do the validation by themselves by implementing a custom `ChannelInboundHandler` that is put in the `ChannelPipeline` behind `Http2StreamFrameToHttpObjectCodec`.

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

CVSSv2:
- Base Score: LOW (2.6)
- Vector: /AV:N/AC:H/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://github.com/netty/netty/security/advisories/GHSA-wm47-8v5p-wjpj
- CONFIRM - https://security.netapp.com/advisory/ntap-20210604-0003/
- DEBIAN - DSA-4885
- MISC - https://github.com/Netflix/zuul/pull/980
- MISC - https://github.com/netty/netty/commit/89c241e3b1795ff257af4ad6eadc616cb2fb3dc4
- MISC - https://lists.apache.org/thread.html/r04a3e0d9f53421fb946c60cc54762b7151dc692eb4e39970a7579052@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r16c4b55ac82be72f28adad4f8061477e5f978199d5725691dcc82c24@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r2e93ce23e04c3f0a61e987d1111d0695cb668ac4ec4edbf237bd3e80@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r490ca5611c150d193b320a2608209180713b7c68e501b67b0cffb925@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r57245853c7245baab09eae08728c52b58fd77666538092389cc3e882@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r6d32fc3cd547f7c9a288a57c7f525f5d00a00d5d163613e0d10a23ef@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r8bcaf7821247b1836b10f6a1a3a3212b06272fd4cde4a859de1b78cf@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/r8db1d7b3b9acc9e8d2776395e280eb9615dd7790e1da8c57039963de@%3Cnotifications.zookeeper.apache.org%3E
- MISC - https://lists.apache.org/thread.html/ra96c74c37ed7252f78392e1ad16442bd16ae72a4d6c8db50dd55c88b@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/racc191a1f70a4f13155e8002c61bddef2870b26441971c697436ad5d@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rae198f44c3f7ac5264045e6ba976be1703cff38dcf1609916e50210d@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rb523bb6c60196c5f58514b86a8585c2069a4852039b45de3818b29d2@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rc73b8dd01b1be276d06bdf07883ecd93fe1a01f139a99ef30ba4308c@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rcfc154eb2de23d2dc08a56100341161e1a40a8ea86c693735437e8f2@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rd25c88aad0e76240dd09f0eb34bdab924933946429e068a167adcb73@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rdb4db3f5a9c478ca52a7b164680b88877a5a9c174e7047676c006b2c@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/re4f70b62843e92163fab03b65e2aa8078693293a0c36f1cc260079ed@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/reafc834062486adfc7be5bb8f7b7793be0d33f483678a094c3f9d468@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://lists.apache.org/thread.html/rf87b870a22aa5c77c27900967b518a71a7d954c2952860fce3794b60@%3Ccommits.servicecomb.apache.org%3E
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MLIST - [bookkeeper-issues] 20210330 [GitHub] [bookkeeper] eolivelli opened a new issue #2669: Update Netty to 4.1.60.final
- MLIST - [flink-dev] 20210424 [jira] [Created] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210424 [jira] [Created] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210426 [jira] [Commented] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210426 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210511 [jira] [Commented] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210610 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210618 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [hbase-commits] 20210402 [hbase-thirdparty] branch master updated: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295 (#48)
- MLIST - [hbase-dev] 20210402 [jira] [Created] (HBASE-25728) [hbase-thirdparty] ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [GitHub] [hbase-thirdparty] Apache-HBase commented on pull request #48: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [GitHub] [hbase-thirdparty] HorizonNet commented on pull request #48: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [GitHub] [hbase-thirdparty] apurtell commented on pull request #48: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [GitHub] [hbase-thirdparty] apurtell merged pull request #48: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [GitHub] [hbase-thirdparty] apurtell opened a new pull request #48: HBASE-25728 [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [jira] [Assigned] (HBASE-25728) [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [jira] [Created] (HBASE-25728) [hbase-thirdparty] ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [jira] [Updated] (HBASE-25728) [hbase-thirdparty] Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [hbase-issues] 20210402 [jira] [Updated] (HBASE-25728) [hbase-thirdparty] Upgrade Netty library to >= 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [jackrabbit-dev] 20210709 [GitHub] [jackrabbit-oak] blackat opened a new pull request #321: Update netty to resolve CVE-2021-21295 and BDSA-2018-4022
- MLIST - [kafka-dev] 20210330 [jira] [Created] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-dev] 20210401 [jira] [Resolved] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210330 [jira] [Created] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210330 [jira] [Updated] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210331 [GitHub] [kafka] dongjinleekr commented on pull request #10448: KAFKA-12583: Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210331 [GitHub] [kafka] dongjinleekr opened a new pull request #10448: KAFKA-12583: Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210401 [jira] [Commented] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210401 [jira] [Resolved] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210402 [jira] [Assigned] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kudu-issues] 20210904 [jira] [Created] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60

- MLIST - [kudu-issues] 20210904 [jira] [Updated] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210907 [jira] [Commented] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210907 [jira] [Resolved] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210907 [jira] [Updated] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] aahmed-se opened a new pull request #10073: Upgrade Netty version to 4.1.60.final
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] merlimat closed issue #10071: CVE-2021-21295 & CVE-2021-21290
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] yaswanthnadella opened a new issue #10071: CVE-2021-21295 & CVE-2021-21290
- MLIST - [pulsar-commits] 20211020 [GitHub] [pulsar] Shoothzj opened a new pull request #12437: [Security] Bump grpc to 1.41.0
- MLIST - [ranger-dev] 20210317 [jira] [Assigned] (RANGER-3209) Upgrade netty to 4.1.60+ due to CVE-2021-21290 and CVE-2021-21295
- MLIST - [ranger-dev] 20210317 [jira] [Created] (RANGER-3209) Upgrade netty to 4.1.60+ due to CVE-2021-21290 and CVE-2021-21295
- MLIST - [zookeeper-commits] 20210331 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-4272 ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-commits] 20210331 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-commits] 20210331 [zookeeper] branch branch-3.7 updated: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-commits] 20210331 [zookeeper] branch master updated: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-dev] 20210330 [jira] [Created] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-dev] 20210928 [jira] [Created] (ZOOKEEPER-4390) CVE-2021-28169 - Upgrade jetty to 9.4.42
- MLIST - [zookeeper-issues] 20210330 [jira] [Created] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210330 [jira] [Updated] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210331 [jira] [Assigned] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210331 [jira] [Commented] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210331 [jira] [Resolved] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210331 [jira] [Updated] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210401 [jira] [Commented] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210402 [jira] [Commented] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210928 [jira] [Created] (ZOOKEEPER-4390) CVE-2021-28169 - Upgrade jetty to 9.4.42
- MLIST - [zookeeper-issues] 20210928 [jira] [Updated] (ZOOKEEPER-4390) CVE-2021-28169 , - Upgrade jetty to 9.4.42
- MLIST - [zookeeper-issues] 20210928 [jira] [Updated] (ZOOKEEPER-4390) CVE-2021-28169 , CVE-2021-28163, - Upgrade jetty to 9.4.42
- MLIST - [zookeeper-issues] 20210928 [jira] [Updated] (ZOOKEEPER-4390) CVE-2021-28169 , CVE-2021-28163, CVE-2021-34428- Upgrade jetty to 9.4.42
- MLIST - [zookeeper-issues] 20210928 [jira] [Updated] (ZOOKEEPER-4390) CVE-2021-28169 - Upgrade jetty to 9.4.42
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] arshadmohammad closed pull request #1670: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] arshadmohammad commented on pull request #1669: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] arshadmohammad commented on pull request #1670: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] asfgit closed pull request #1669: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] ayushmantri opened a new pull request #1669: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] ayushmantri opened a new pull request #1670: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-notifications] 20210331 [GitHub] [zookeeper] eolivelli commented on pull request #1669: ZOOKEEPER-4272: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.60
- ...

CVE-2021-21409 suppress

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.61.Final there is a vulnerability that enables request smuggling. The content-length header is not correctly validated if the request only uses a single Http2HeaderFrame with the endStream set to to true. This could lead to request smuggling if the request is proxied to a remote peer and translated to HTTP/1.1. This is a followup of GHSA-wm47-8v5p-wjpj/CVE-2021-21295 which did miss to fix this one case. This was fixed as part of 4.1.61.Final.

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

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

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://github.com/netty/netty/security/advisories/GHSA-f256-j965-7f32
- CONFIRM - https://security.netapp.com/advisory/ntap-20210604-0003/
- DEBIAN - DSA-4885
- MISC - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21295
- MISC - https://github.com/netty/netty/commit/b0fa4d5aab4215f3c22ce6123dd8dd5f38dc0432
- MISC - https://github.com/netty/netty/security/advisories/GHSA-wm47-8v5p-wjpj
- 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 - [flink-dev] 20210424 [jira] [Created] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210424 [jira] [Created] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210426 [jira] [Commented] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210426 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210511 [jira] [Commented] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210610 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [flink-issues] 20210618 [jira] [Updated] (FLINK-22441) In Flink v1.11.3 contains netty(version:3.10.6) netty(version:4.1.60) . There are many vulnerabilities, like CVE-2021-21409 etc. please confirm these version and fix. thx
- MLIST - [kafka-jira] 20210506 [GitHub] [kafka] dongjinleekr opened a new pull request #10642: KAFKA-12756: Update Zookeeper to 3.6.3 or higher
- MLIST - [kudu-issues] 20210904 [jira] [Created] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210904 [jira] [Updated] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210907 [jira] [Commented] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60

- MLIST - [kudu-issues] 20210907 [jira] [Resolved] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [kudu-issues] 20210907 [jira] [Updated] (KUDU-3313) There is a CVE-2021-21409 vulnerability in netty version 4.1.60
- MLIST - [pulsar-commits] 20210419 [GitHub] [pulsar] lhotari commented on pull request #10266: [Security] Upgrade Netty to 4.1.63.Final to address CVE-2021-21409
- MLIST - [pulsar-commits] 20210419 [GitHub] [pulsar] lhotari opened a new pull request #10266: [Security] Upgrade Netty to 4.1.63.Final to address CVE-2021-21409
- MLIST - [pulsar-commits] 20210420 [GitHub] [pulsar] eolivelli merged pull request #10266: [Security] Upgrade Netty to 4.1.63.Final to address CVE-2021-21409
- MLIST - [pulsar-commits] 20211020 [GitHub] [pulsar] Shoothzj opened a new pull request #12437: [Security] Bump grpc to 1.41.0
- MLIST - [zookeeper-commits] 20210408 [zookeeper] 01/02: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-commits] 20210408 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-commits] 20210408 [zookeeper] branch branch-3.7 updated: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-commits] 20210408 [zookeeper] branch master updated: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-commits] 20210924 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-4385. Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-dev] 20210407 [jira] [Created] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-dev] 20210517 [jira] [Created] (ZOOKEEPER-4295) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21409 in branch-3.5
- MLIST - [zookeeper-dev] 20210923 [jira] [Created] (ZOOKEEPER-4385) Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-issues] 20210407 [jira] [Assigned] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210407 [jira] [Created] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210408 [jira] [Assigned] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210408 [jira] [Comment Edited] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210408 [jira] [Commented] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210408 [jira] [Resolved] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210408 [jira] [Updated] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210409 [jira] [Commented] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210517 [jira] [Created] (ZOOKEEPER-4295) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21409 in branch-3.5
- MLIST - [zookeeper-issues] 20210517 [jira] [Updated] (ZOOKEEPER-4295) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21409 in branch-3.5
- MLIST - [zookeeper-issues] 20210727 [jira] [Comment Edited] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210727 [jira] [Commented] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210922 [jira] [Commented] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210923 [jira] [Assigned] (ZOOKEEPER-4385) Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-issues] 20210923 [jira] [Commented] (ZOOKEEPER-4278) dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-issues] 20210923 [jira] [Created] (ZOOKEEPER-4385) Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-issues] 20210923 [jira] [Updated] (ZOOKEEPER-4385) Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-issues] 20210924 [jira] [Resolved] (ZOOKEEPER-4385) Backport ZOOKEEPER-4278 to branch-3.5 to Address CVE-2021-21409
- MLIST - [zookeeper-notifications] 20210408 [GitHub] [zookeeper] arshadmohammad commented on pull request #1678: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-notifications] 20210408 [GitHub] [zookeeper] asfgit closed pull request #1678: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-notifications] 20210408 [GitHub] [zookeeper] ayushmantri opened a new pull request #1678: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- MLIST - [zookeeper-notifications] 20210517 [GitHub] [zookeeper] gpiyush-dev opened a new pull request #1696: ZOOKEEPER-4295: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21409 in branch-3.5
- MLIST - [zookeeper-notifications] 20210521 [GitHub] [zookeeper] maoling commented on pull request #1696: ZOOKEEPER-4295: Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21409 in branch-3.5
- MLIST - [zookeeper-notifications] 20210727 [GitHub] [zookeeper] sandipbhattacharya commented on pull request #1678: ZOOKEEPER-4278: dependency-check:check failing - netty-transport-4.1.60.Final CVE-2021-21409
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.61
- ...

CVE-2021-21290 suppress

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty before version 4.1.59.Final there is a vulnerability on Unix-like systems involving an insecure temp file. When netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method "File.createTempFile" on unix-like systems creates a random file, but, by default will create this file with the permissions "-rw-r--r--". Thus, if sensitive information is written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59.Final. As a workaround, one may specify your own "java.io.tmpdir" when you start the JVM or use "DefaultHttpDataFactory.setBaseDir(...)" to set the directory to something that is only readable by the current user.

CWE-378 Creation of Temporary File With Insecure Permissions, CWE-379 Creation of Temporary File in Directory with Incorrect Permissions

CVSSv2:
- Base Score: LOW (1.9)
- Vector: /AV:L/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://github.com/netty/netty/security/advisories/GHSA-5mcr-gq6c-3hq2
- CONFIRM - https://security.netapp.com/advisory/ntap-20220210-0011/
- DEBIAN - DSA-4885
- MISC - https://github.com/netty/netty/commit/c735357bf29d07856ad171c6611a2e1a0e0000ec
- MISC - https://lists.apache.org/thread.html/r0053443ce19ff125981559f8c51cf66e3ab4350f47812b8cf0733a05@%3Cdev.kafka.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/cpuoct2021.html
- MLIST - [activemq-users] 20210715 Next ActiveMQ Artemis Release - CVE-2021-21290 vulnerability
- MLIST - [bookkeeper-issues] 20210330 [GitHub] [bookkeeper] eolivelli opened a new issue #2669: Update Netty to 4.1.60.final
- MLIST - [debian-lts-announce] 20210211 [SECURITY] [DLA 2555-1] netty security update
- MLIST - [kafka-commits] 20210302 [kafka] branch 2.6 updated: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-commits] 20210302 [kafka] branch 2.7 updated: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-dev] 20210301 [jira] [Created] (KAFKA-12389) Upgrade of netty-codec due to CVE-2021-21290

- MLIST - [kafka-dev] 20210302 [jira] [Resolved] (KAFKA-12389) Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-dev] 20210330 [jira] [Created] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210301 [GitHub] [kafka] dongjinleekr commented on pull request #10235: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210301 [GitHub] [kafka] dongjinleekr opened a new pull request #10235: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210301 [jira] [Assigned] (KAFKA-12389) Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210301 [jira] [Created] (KAFKA-12389) Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210302 [GitHub] [kafka] dongjinleekr commented on pull request #10235: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210302 [GitHub] [kafka] omkreddy closed pull request #10235: KAFKA-12389: Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210302 [jira] [Resolved] (KAFKA-12389) Upgrade of netty-codec due to CVE-2021-21290
- MLIST - [kafka-jira] 20210330 [jira] [Created] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [kafka-jira] 20210330 [jira] [Updated] (KAFKA-12583) Upgrade of netty-codec due to CVE-2021-21295
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] aahmed-se opened a new pull request #10073: Upgrade Netty version to 4.1.60.final
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] merlimat closed issue #10071: CVE-2021-21295 & CVE-2021-21290
- MLIST - [pulsar-commits] 20210329 [GitHub] [pulsar] yaswanthnadella opened a new issue #10071: CVE-2021-21295 & CVE-2021-21290
- MLIST - [pulsar-commits] 20211020 [GitHub] [pulsar] Shoothzj opened a new pull request #12437: [Security] Bump grpc to 1.41.0
- MLIST - [ranger-dev] 20210317 [jira] [Assigned] (RANGER-3209) Upgrade netty to 4.1.60+ due to CVE-2021-21290 and CVE-2021-21295
- MLIST - [ranger-dev] 20210317 [jira] [Created] (RANGER-3209) Upgrade netty to 4.1.60+ due to CVE-2021-21290 and CVE-2021-21295
- MLIST - [tinkerpop-dev] 20210316 [jira] [Created] (TINKERPOP-2535) Netty 4.1.52 flagged as medium security violation
- MLIST - [zookeeper-dev] 20210311 [jira] [Created] (ZOOKEEPER-4242) Upgrade Netty library to > 4.1.59 due to security vulnerability
- MLIST - [zookeeper-dev] 20210330 [jira] [Created] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210311 [jira] [Created] (ZOOKEEPER-4242) Upgrade Netty library to > 4.1.59 due to security vulnerability
- MLIST - [zookeeper-issues] 20210330 [jira] [Created] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210330 [jira] [Updated] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- MLIST - [zookeeper-issues] 20210402 [jira] [Commented] (ZOOKEEPER-4272) Upgrade Netty library to > 4.1.60 due to security vulnerability CVE-2021-21295
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.59
- ...

CVE-2022-24823 suppress

Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codec-http` prior to version 4.1.77.Final contains an insufficient fix for CVE-2021-21290. When Netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. This only impacts applications running on Java version 6 and lower. Additionally, this vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they all share the system temporary directory between all users. Version 4.1.77.Final contains a patch for this vulnerability. As a workaround, specify one's own `java.io.tmpdir` when starting the JVM or use DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.

CWE-378 Creation of Temporary File With Insecure Permissions, CWE-379 Creation of Temporary File in Directory with Incorrect Permissions, CWE-668 Exposure of Resource to Wrong Sphere

CVSSv2:
- Base Score: LOW (1.9)
- Vector: /AV:L/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://github.com/netty/netty/security/advisories/GHSA-269q-hmxg-m83q
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0004/
- MISC - https://github.com/netty/netty/commit/185f8b2756a36aaa4f973f1a2a025e7d981823f1
- MISC - https://github.com/netty/netty/security/advisories/GHSA-5mcr-gg6c-3hq2
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:netty:netty:*:*:*:*:*:*:*:* versions up to (excluding) 4.1.77
- ...

postgresql-42.2.16.jar

Description:

PostgreSQL JDBC Driver Postgresql

License:

BSD-2-Clause: https://jdbc.postgresql.org/about/license.html

File Path: /Users/djvelickovic/.m2/repository/org/postgresql/postgresql/42.2.16/postgresql-42.2.16.jar
MD5: 6d02942406e92153c6675617dade3524
SHA1: a9ee12f737bd5dc7d046e4c065e391d38d6a3cfc
SHA256:82230367c0e9507be45981ce2aa059f7291d906f56ad820d0bab3db0cf1523cb
Referenced In Project/Scope: engine:runtime
Included by: pkg:maven/io.isotope.enigma/engine@0.0.1-SNAPSHOT

Evidence

Identifiers

- pkg:maven/org.postgresql/postgresql@42.2.16 (*Confidence*:High)
- cpe:2.3:a:postgresql:postgresql_jdbc_driver:42.2.16:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2022-21724 suppress

pgjdbc is the offical PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue.

CWE-665 Improper Initialization

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

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

References:
- CONFIRM - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-v7wg-cpwc-24m4
- CONFIRM - https://security.netapp.com/advisory/ntap-20220311-0005/
- DEBIAN - DSA-5196
- FEDORA - FEDORA-2022-1151f65e9a
- MISC - https://github.com/pgjdbc/pgjdbc/commit/f4d0ed69c0b3aae8531d83d6af4c57f22312c813
- MLIST - [debian-lts-announce] 20220520 [SECURITY] [DLA 3018-1] libpgjava security update
- OSSINDEX - [CVE-2022-21724] CWE-665: Improper Initialization
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21724
- OSSIndex - https://github.com/advisories/GHSA-v7wg-cpwc-24m4
- OSSIndex - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-v7wg-cpwc-24m4

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:*:*:* versions up to (excluding) 42.2.25
- ...

CVE-2022-26520 (OSSINDEX) suppress

** DISPUTED ** In pgjdbc before 42.3.3, an attacker (who controls the jdbc URL or properties) can call java.util.logging.FileHandler to write to arbitrary files through the loggerFile and loggerLevel connection properties. An example situation is that an attacker could create an executable JSP file under a Tomcat web root. NOTE: the vendor's position is that there is no pgjdbc vulnerability; instead, it is a vulnerability for any application to use the pgjdbc driver with untrusted connection properties.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2022-26520 for details

CWE-20 Improper Input Validation

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

References:
- OSSINDEX - [CVE-2022-26520] CWE-20: Improper Input Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26520
- OSSIndex - https://github.com/pgjdbc/pgjdbc/pull/2454
- OSSIndex - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-673j-qm5f-xpv8
- OSSIndex - https://jdbc.postgresql.org/documentation/changelog.html#version_42.3.3

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.postgresql:postgresql:42.2.16:*:*:*:*:*:*:*

CVE-2022-31197 suppress

PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue.

CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CVSSv3:
- Base Score: HIGH (8.0)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-r38f-c4h4-hqq2
- FEDORA - FEDORA-2022-cdeabe1bc0
- FEDORA - FEDORA-2022-d7d49b2fac
- MISC - https://github.com/pgjdbc/pgjdbc/commit/739e599d52ad80f8dcd6efedc6157859b1a9d637
- MLIST - [debian-lts-announce] 20221008 [SECURITY] [DLA 3140-1] libpgjava security update

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:*:*:* versions up to (excluding) 42.2.26
- ...

CVE-2022-41946 suppress

pgjdbc is an open source postgresql JDBC Driver. In affected versions a prepared statement using either `PreparedStatement.setText(int, InputStream)` or `PreparedStatemet.setBytea(int, InputStream)` will create a temporary file if the InputStream is larger than 2k. This will create a temporary file which is readable by other

users on Unix like systems, but not MacOS. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. Java 1.7 and higher users: this vulnerability is fixed in 4.5.0. Java 1.6 and lower users: no patch is available. If you are unable to patch, or are stuck running on Java 1.6, specifying the java.io.tmpdir system environment variable to a directory that is exclusively owned by the executing user will mitigate this vulnerability.

CWE-200 Information Exposure, CWE-377 Insecure Temporary File

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h
- FEDORA - FEDORA-2023-42d6ba9bd6
- MISC - https://github.com/pgjdbc/pgjdbc/commit/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5
- MLIST - [debian-lts-announce] 20221202 [SECURITY] [DLA 3218-1] libpgjava security update
- OSSINDEX - [CVE-2022-41946] CWE-200: Information Exposure
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41946
- OSSIndex - https://github.com/advisories/GHSA-562r-vg33-8x8h
- OSSIndex - https://github.com/pgjdbc/pgjdbc/blob/9008dc9aade6dbfe4efafcd6872ebc55f4699cf5/CHANGELOG.md#security
- OSSIndex - https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-562r-vg33-8x8h

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:postgresql:postgresql_jdbc_driver:*:*:*:*:*:*:*:* versions from (including) 42.2.0; versions up to (excluding) 42.2.27
- ...

reactor-netty-0.9.12.RELEASE.jar

Description:

Reactive Streams Netty driver

License:

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

File Path: /Users/djvelickovic/.m2/repository/io/projectreactor/netty/reactor-netty/0.9.12.RELEASE/reactor-netty-0.9.12.RELEASE.jar
MD5: ac11194278f0981915639f9c5bc9b013
SHA1: 41022546d07f1499fb9d8617bba4a1a89d3549db
SHA256:951b18e6ba8786b79ed0f39974d1b6d00b3d900e8d1472e10014d0a4d70827f3
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-webflux@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/io.projectreactor.netty/reactor-netty@0.9.12.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal:reactor_netty:0.9.12:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-31684 (OSSINDEX) suppress

Reactor Netty HTTP Server, in versions 1.0.11 - 1.0.23, may log request headers in some cases of invalid HTTP requests. The logged headers may reveal valid access tokens to those with access to server logs. This may affect only invalid HTTP requests where logging at WARN level is enabled.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2022-31684 for details

CWE-200 Information Exposure

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

References:
- OSSINDEX - [CVE-2022-31684] CWE-200: Information Exposure
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-31684
- OSSIndex - https://github.com/reactor/reactor-netty/pull/2528
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-31684

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:io.projectreactor.netty:reactor-netty:0.9.12.RELEASE:*:*:*:*:*:*:*

snakeyaml-1.26.jar

Description:

YAML 1.1 parser and emitter for Java

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/yaml/snakeyaml/1.26/snakeyaml-1.26.jar
MD5: 72d987f6193910b63c5e6881ab64da32
SHA1: a78a8747147d2c5807683e76ec2b633e95c14fe9
SHA256:d87d607e500885356c03c1cae61e8c2e05d697df8787d5aba13484c2eb76a844
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.yaml/snakeyaml@1.26 (*Confidence*:High)
- cpe:2.3:a:snakeyaml_project:snakeyaml:1.26:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-1471 (OSSINDEX) 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.

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-2022-1471] CWE-502: Deserialization of Untrusted Data
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1471
- OSSIndex - https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.yaml:snakeyaml:1.26:*:*:*:*:*:*:*

CVE-2022-25857 suppress

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

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

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

References:
- 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-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-25857
- OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/525

Vulnerable Software & Versions:

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

CVE-2022-38749 suppress

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

CWE-787 Out-of-bounds Write

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38749
- OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/525

- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47024

Vulnerable Software & Versions:

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

CVE-2022-38751 suppress

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

CWE-787 Out-of-bounds Write

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38751
- OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/530/stackoverflow-oss-fuzz-47039
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47039

Vulnerable Software & Versions:

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

CVE-2022-38752 suppress

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

CWE-787 Out-of-bounds Write

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38752
- OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/531/stackoverflow-oss-fuzz-47081
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47081
- OSSIndex - https://github.com/advisories/GHSA-9w3m-gqgf-c4p9

Vulnerable Software & Versions:

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

CVE-2022-41854 suppress

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

CWE-787 Out-of-bounds Write

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References:
- CONFIRM - N/A
- FEDORA - FEDORA-2022-8a4e8aa190
- FEDORA - FEDORA-2022-c01dd659fa
- OSSINDEX - [CVE-2022-41854] CWE-787: Out-of-bounds Write
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41854
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355

Vulnerable Software & Versions:

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

CVE-2022-38750 suppress

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

CWE-787 Out-of-bounds Write

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

References:
- 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
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38750
- OSSIndex - https://bitbucket.org/snakeyaml/snakeyaml/issues/526/stackoverflow-oss-fuzz-47027
- OSSIndex - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47027

Vulnerable Software & Versions:

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

spring-boot-2.3.4.RELEASE.jar

Description:

Spring Boot

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/boot/spring-boot/2.3.4.RELEASE/spring-boot-2.3.4.RELEASE.jar
MD5: d344958f6acd622e442372aaa02953a9
SHA1: f23f14ae4062d5983db89b7c7336166b6734fc57
SHA256:6f31d29d22fc2003fc77b90db2c028a1e2e8d4e6b2a6ed61b07269aeb1c3d4a9
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.springframework.boot/spring-boot@2.3.4.RELEASE (*Confidence*:High)
- cpe:2.3:a:vmware:spring_boot:2.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-27772 (OSSINDEX) suppress

** UNSUPPORTED WHEN ASSIGNED ** 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.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2022-27772 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-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772
- OSSIndex - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- OSSIndex - https://github.com/github/codeql/pull/4473#issuecomment-1030416237
- OSSIndex - https://github.com/spring-projects/spring-boot/issues/23622

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework.boot:spring-boot:2.3.4.RELEASE:*:*:*:*:*:*:*:*

spring-boot-container-bundle-11.0.2.jar

File Path: /Users/djvelickovic/.m2/repository/org/keycloak/spring-boot-container-bundle/11.0.2/spring-boot-container-bundle-11.0.2.jar
MD5: 930105b71cb56dc37af26492b1ecdf6c
SHA1: 2c5a4a8575f2065fa45ffdb314215470d7771998
SHA256:5a1a6c12ec533e312dff59f1a9302bac5e7bcdbfb07916b444318fa511360fa1
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.keycloak/keycloak-spring-boot-starter@11.0.2

Evidence

Identifiers

- pkg:maven/org.keycloak/spring-boot-container-bundle@11.0.2 (*Confidence*:High)
- cpe:2.3:a:keycloak:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:redhat:keycloak:11.0.2:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-1245 suppress

A privilege escalation flaw was found in the token exchange feature of keycloak. Missing authorization allows a client application holding a valid access token to exchange tokens for any target client by passing the client_id of the target. This could allow a client to gain unauthorized access to additional services.

CWE-862 Missing Authorization

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

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

References:
- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-75p6-52g3-rqc8

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0

CVE-2021-20195 suppress

A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CWE-116 Improper Encoding or Escaping of Output

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

CVSSv3:
- Base Score: CRITICAL (9.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1919143

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.3

CVE-2020-14389 suppress

It was found that Keycloak before version 12.0.0 would permit a user with only view-profile role to manage the resources in the new account console, allowing access and modification of data the user was not intended to have.

CWE-916 Use of Password Hash With Insufficient Computational Effort

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- MISC - https://access.redhat.com/security/cve/cve-2020-14389
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1875843,

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2020-14366 suppress

A vulnerability was found in keycloak, where path traversal using URL-encoded path segments in the request is possible because the resources endpoint applies a transformation of the url path to the file path. Only few specific folder hierarchies can be exposed by this flaw

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

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

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

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14366

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-20222 suppress

A flaw was found in keycloak. The new account console in keycloak can allow malicious code to be executed using the referrer URL. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

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

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1924606

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions from (including) 9.0.0; versions up to (excluding) 13.0.0

CVE-2021-3513 suppress

A flaw was found in keycloak where a brute force attack is possible even when the permanent lockout feature is enabled. This is due to a wrong error message displayed when wrong credentials are entered. The highest threat from this vulnerability is to confidentiality.

CWE-209 Information Exposure Through an Error Message

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3513
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1953439

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3632 suppress

A flaw was found in Keycloak. This vulnerability allows anyone to register a new security device or key when there is not a device already registered for any user by using the WebAuthn password-less login flow.

CWE-287 Improper Authentication

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

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3632
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1978196
- MISC - https://github.com/keycloak/keycloak/commit/65480cb5a11630909c086f79d396004499fbd1e4
- MISC - https://github.com/keycloak/keycloak/pull/8203
- MISC - https://issues.redhat.com/browse/KEYCLOAK-18500

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0
- ...

CVE-2021-3637 suppress

A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1979638

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 14.0.0
- ...

CVE-2021-20202 suppress

A flaw was found in keycloak. Directories can be created prior to the Java process creating them in the temporary directory, but with wider user permissions, allowing the attacker to have access to the contents that keycloak stores in this directory. The highest threat from this vulnerability is to data confidentiality and integrity.

CWE-377 Insecure Temporary File

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

CVSSv3:
- Base Score: HIGH (7.3)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1922128

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2021-3827 suppress

A flaw was found in keycloak, where the default ECP binding flow allows other authentication flows to be bypassed. By exploiting this behavior, an attacker can bypass the MFA authentication by sending a SOAP request with an AuthnRequest and Authorization header with the user's credentials. The highest threat from this vulnerability is to confidentiality and integrity.

CWE-287 Improper Authentication

CVSSv3:
- Base Score: MEDIUM (6.8)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- MISC - https://access.redhat.com/security/cve/CVE-2021-3827
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2007512
- MISC - https://github.com/keycloak/keycloak/commit/44000caaf5051d7f218d1ad79573bd3d175cad0d
- MISC - https://github.com/keycloak/keycloak/security/advisories/GHSA-4pc7-vqv5-5r3v

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 18.0.0
- ...

CVE-2020-27838 suppress

A flaw was found in keycloak in versions prior to 13.0.0. The client registration endpoint allows fetching information about PUBLIC clients (like client secret) without authentication which could be an issue if the same PUBLIC client changed to CONFIDENTIAL later. The highest threat from this vulnerability is to data confidentiality.

CWE-287 Improper Authentication

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1906797

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0
- ...

CVE-2022-1466 suppress

Due to improper authorization, Red Hat Single Sign-On is vulnerable to users performing actions that they should not be allowed to perform. It was possible to add users to the master realm even though no respective permission was granted.

CWE-863 Incorrect Authorization

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2050228
- MISC - https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-076.txt
- MISC - https://www.syss.de/pentest-blog/fehlerhafte-autorisierung-bei-red-hat-single-sign-on-750ga-syss-2021-076

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.1
- ...

CVE-2021-20323 suppress

A POST based reflected Cross Site Scripting vulnerability on has been identified in Keycloak.

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

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2013577

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 17.0.0

CVE-2020-1725 suppress

A flaw was found in keycloak before version 13.0.0. In some scenarios a user still has access to a resource after changing the role mappings in Keycloak and after

expiration of the previous access token.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1765129
- MISC - https://issues.redhat.com/browse/KEYCLOAK-16550

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10770 suppress

A flaw was found in Keycloak before 13.0.0, where it is possible to force the server to call out an unverified URL using the OIDC parameter request_uri. This flaw allows an attacker to use this parameter to execute a Server-side request forgery (SSRF) attack.

CWE-918 Server-Side Request Forgery (SSRF)

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - http://packetstormsecurity.com/files/164499/Keycloak-12.0.1-Server-Side-Request-Forgery.html
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1846270

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.2

CVE-2020-14302 suppress

A flaw was found in Keycloak before 13.0.0 where an external identity provider, after successful authentication, redirects to a Keycloak endpoint that accepts multiple invocations with the use of the same "state" parameter. This flaw allows a malicious user to perform replay attacks.

CWE-294 Authentication Bypass by Capture-replay

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

CVSSv3:
- Base Score: MEDIUM (4.9)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1849584

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 13.0.0

CVE-2020-10776 suppress

A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack.

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

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

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1847428

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0

CVE-2021-3856 suppress

ClassLoaderTheme and ClasspathThemeResourceProviderFactory allows reading any file available as a resource to the classloader. By sending requests for theme resources with a relative path from an external HTTP client, the client will receive the content of random files if available.

CWE-552 Files or Directories Accessible to External Parties

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:

- MISC - https://access.redhat.com/security/cve/CVE-2021-3856
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=2010164
- MISC - https://github.com/keycloak/keycloak/commit/73f0474008e1bebd0733e62a22aceda9e5de6743
- MISC - https://github.com/keycloak/keycloak/pull/8588
- MISC - https://issues.redhat.com/browse/KEYCLOAK-19422

Vulnerable Software & Versions:

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 15.1.0

CVE-2020-27826 suppress

A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker to change its own NameID attribute to impersonate the admin user for any particular application.

CWE-250 Execution with Unnecessary Privileges

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.2)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1905089

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:redhat:keycloak:*:*:*:*:*:*:*:* versions up to (excluding) 12.0.0
- ...

spring-core-5.2.9.RELEASE.jar

Description:

Spring Core

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/spring-core/5.2.9.RELEASE/spring-core-5.2.9.RELEASE.jar
MD5: a063b16385dbeee24b99dad07bb4ae1f
SHA1: 400a6fdb45bfa5318aa7d06360f4495b75080bb5
SHA256:7cbae8ae5ccf5f238b101596c6a6d87e9451d98fbd9c4a6af1dac49cf1c0538a
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-test@2.3.4.RELEASE

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.springframework/spring-core@5.2.9.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-22965 suppress

CISA Known Exploited Vulnerability:
- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25

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

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

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

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

References:
- CISCO - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- CONFIRM - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- MISC - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- MISC - https://tanzu.vmware.com/security/cve-2022-22965
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- N/A - N/A
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSINDEX - [sonatype-2022-1764] CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

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

CVE-2021-22118 suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210713-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22118
- 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-2021-22118] CWE-668: Exposure of Resource to Wrong Sphere
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118

Vulnerable Software & Versions: (show all)

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

CVE-2022-22950 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://tanzu.vmware.com/security/cve-2022-22950
- OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28145
- OSSIndex - https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22971 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:
- Base Score: MEDIUM (4.0)

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22971
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

CVE-2022-22968 suppress

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

CWE-178 Improper Handling of Case Sensitivity

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220602-0004/
- MISC - https://tanzu.vmware.com/security/cve-2022-22968
- N/A - N/A
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

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

CVE-2022-22970 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0006/
- MISC - https://tanzu.vmware.com/security/cve-2022-22970
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

CVE-2021-22060 suppress

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

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22060
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22060] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22060

Vulnerable Software & Versions: (show all)

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

CVE-2021-22096 suppress

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

NVD-CWE-Other

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20211125-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22096
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22096

Vulnerable Software & Versions: (show all)

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

spring-security-core-5.3.4.RELEASE.jar

Description:

spring-security-core

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/security/spring-security-core/5.3.4.RELEASE/spring-security-core-5.3.4.RELEASE.jar
MD5: 19e53c47622be720b08bcb27e8d73290
SHA1: 81a2fc0900726aa480f51f2a43392ed60c2e4425
SHA256:b227c346b807dda45f4144e21df58560a2810af0c03dbbcb73e3119d3269608b
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-security@2.3.4.RELEASE

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.springframework.security/spring-security-core@5.3.4.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_security:5.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_security:5.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-22978 suppress

In Spring Security versions 5.5.6 and 5.6.3 and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass

CWE-863 Incorrect Authorization

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220707-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22978
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions up to (excluding) 5.5.7
- ...

CVE-2021-22112 suppress

Spring Security 5.4.x prior to 5.4.4, 5.3.x prior to 5.3.8.RELEASE, 5.2.x prior to 5.2.9.RELEASE, and older unsupported versions can fail to save the SecurityContext if it is changed more than once in a single request.A malicious user cannot cause the bug to happen (it must be programmed in). However, if the application's intent is to only allow the user to run with elevated privileges in a small portion of the application, the bug can be leveraged to extend those privileges to the rest of the application.

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (9.0)
- Vector: /AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22112
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [nifi-issues] 20210510 [GitHub] [nifi] exceptionfactory opened a new pull request #5066: NIFI-8502 Upgrade Spring Framework to 5.3.6
- MLIST - [oss-security] 20210219 Vulnerability in Jenkins
- MLIST - [portals-pluto-dev] 20210623 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210623 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Comment Edited] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-scm] 20210623 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:pivotal_software:spring_security:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.8
- ...

CVE-2021-22119 suppress

Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client Web and WebFlux application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session or multiple sessions.

CWE-863 Incorrect Authorization

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

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

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22119
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [nifi-issues] 20210726 [jira] [Created] (NIFI-8948) Upgrade Spring Framework to 5.3.9 and Spring Security to 5.5.1
- MLIST - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Comment Edited] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.10
- ...

CVE-2022-22976 suppress

Spring Security versions 5.5.x prior to 5.5.7, 5.6.x prior to 5.6.4, and earlier unsupported versions contain an integer overflow vulnerability. When using the BCrypt class with the maximum work factor (31), the encoder does not perform any salt rounds, due to an integer overflow error. The default settings are not affected by this CVE.

CWE-190 Integer Overflow or Wraparound

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220707-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22976

- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions up to (excluding) 5.5.7
- ...

spring-security-web-5.3.4.RELEASE.jar

Description:

spring-security-web

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/security/spring-security-web/5.3.4.RELEASE/spring-security-web-5.3.4.RELEASE.jar
MD5: 1c2052d4ada65bb3d5bab4b816dbba1f
SHA1: 9574a39bd514ece4cb8cfcb4e05c0ee2c5b53046
SHA256:bac619908d96d79ef20375b430a451d8c782f1bd11295c57bf40e1accdfca273
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-security@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.springframework.security/spring-security-web@5.3.4.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_security:5.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_security:5.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:web_project:web:5.3.4:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-22978 suppress

In Spring Security versions 5.5.6 and 5.6.3 and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass

CWE-863 Incorrect Authorization

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220707-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22978
- N/A - N/A
- OSSINDEX - [CVE-2022-22978] CWE-863: Incorrect Authorization
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22978
- OSSIndex - https://spring.io/blog/2022/05/15/cve-2022-22978-authorization-bypass-in-regexrequestmatcher

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions up to (excluding) 5.5.7
- ...

CVE-2021-22112 suppress

Spring Security 5.4.x prior to 5.4.4, 5.3.x prior to 5.3.8.RELEASE, 5.2.x prior to 5.2.9.RELEASE, and older unsupported versions can fail to save the SecurityContext if it is changed more than once in a single request.A malicious user cannot cause the bug to happen (it must be programmed in). However, if the application's intent is to only allow the user to run with elevated privileges in a small portion of the application, the bug can be leveraged to extend those privileges to the rest of the application.

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (9.0)
- Vector: /AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22112
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [nifi-issues] 20210510 [GitHub] [nifi] exceptionfactory opened a new pull request #5066: NIFI-8502 Upgrade Spring Framework to 5.3.6

- MLIST - [oss-security] 20210219 Vulnerability in Jenkins
- MLIST - [portals-pluto-dev] 20210623 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210623 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Comment Edited] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-scm] 20210623 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.0 due to CVE-2021-22112
- MLIST - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- N/A - N/A
- OSSINDEX - [CVE-2021-22112] CWE-285: Improper Authorization
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22112
- OSSIndex - https://github.com/spring-projects/spring-security/issues/9387
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22112

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:pivotal_software:spring_security:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.8
- ...

CVE-2021-22119 suppress

Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client Web and WebFlux application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session or multiple sessions.

CWE-863 Incorrect Authorization

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

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

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22119
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MLIST - [nifi-issues] 20210726 [jira] [Created] (NIFI-8948) Upgrade Spring Framework to 5.3.9 and Spring Security to 5.5.1
- MLIST - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Comment Edited] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Reopened] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-dev] 20210714 [jira] [Updated] (PLUTO-786) Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- MLIST - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-786 Upgrade to version Spring Framework 5.3.7 and Spring Security 5.5.1 due to CVE-2021-22112 and CVE-2021-22119
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions from (including) 5.3.0; versions up to (excluding) 5.3.10
- ...

CVE-2022-22976 suppress

Spring Security versions 5.5.x prior to 5.5.7, 5.6.x prior to 5.6.4, and earlier unsupported versions contain an integer overflow vulnerability. When using the BCrypt class with the maximum work factor (31), the encoder does not perform any salt rounds, due to an integer overflow error. The default settings are not affected by this CVE.

CWE-190 Integer Overflow or Wraparound

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220707-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22976
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:* versions up to (excluding) 5.5.7
- ...

spring-web-5.2.9.RELEASE.jar

Description:

Spring Web

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/spring-web/5.2.9.RELEASE/spring-web-5.2.9.RELEASE.jar
MD5: 0e08df30bdd6cf91ef40ab8155cb4768
SHA1: 4bc4a60b74ea0a92ed09d41c675f8426324b4e56
SHA256:76355c69937b0e8153169608532e8424cec029f51687f193bf72eb1ca109e7f2
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.springframework/spring-web@5.2.9.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:web_project:web:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2016-1000027 suppress

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

CWE-502 Deserialization of Untrusted Data

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

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

References:
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- MISC - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- MISC - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- MISC - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- MISC - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- MISC - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- MISC - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- MISC - https://www.tenable.com/security/research/tra-2016-20
- OSSINDEX - [CVE-2016-1000027] CWE-502: Deserialization of Untrusted Data
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027
- OSSIndex - https://blog.gypsyengineer.com/en/security/detecting-dangerous-spring-exporters-with-codeql.html
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/24434
- OSSIndex - https://www.tenable.com/security/research/tra-2016-20

Vulnerable Software & Versions:

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

CVE-2022-22965 suppress

CISA Known Exploited Vulnerability:
- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25

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

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

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

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

References:
- CISCO - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022

- CONFIRM - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- CONFIRM - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- MISC - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- MISC - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- MISC - https://tanzu.vmware.com/security/cve-2022-22965
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- N/A - N/A
- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSINDEX - [sonatype-2022-1764] CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

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

CVE-2021-22118 suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210713-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22118
- 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-2021-22118] CWE-668: Exposure of Resource to Wrong Sphere
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118

Vulnerable Software & Versions: (show all)

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

CVE-2022-22950 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://tanzu.vmware.com/security/cve-2022-22950
- OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28145
- OSSIndex - https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22971 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:

- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22971
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

CVE-2022-22968 suppress

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

CWE-178 Improper Handling of Case Sensitivity

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220602-0004/
- MISC - https://tanzu.vmware.com/security/cve-2022-22968
- N/A - N/A
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

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

CVE-2022-22970 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0006/
- MISC - https://tanzu.vmware.com/security/cve-2022-22970
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

CVE-2021-22060 suppress

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

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22060
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22060] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22060

Vulnerable Software & Versions: (show all)

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

CVE-2021-22096 suppress

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

NVD-CWE-Other

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20211125-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22096
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22096

Vulnerable Software & Versions: (show all)

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

spring-webmvc-5.2.9.RELEASE.jar

Description:

Spring Web MVC

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/springframework/spring-webmvc/5.2.9.RELEASE/spring-webmvc-5.2.9.RELEASE.jar
MD5: f3aafd50ceab3c2acce87cdf451eecca
SHA1: bec8682df7622707f067f98457ee95a8f276de80
SHA256:2825194d46c244ff5e64fcba9273bfc8779667a3aac33eb4ea9ef87dfb4fa4ac
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Identifiers

- pkg:maven/org.springframework/spring-webmvc@5.2.9.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:springsource:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:web_project:web:5.2.9:release:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2022-22965 suppress

CISA Known Exploited Vulnerability:
- Product: VMware Spring Framework
- Name: Spring Framework JDK 9+ Remote Code Execution Vulnerability
- Date Added: 2022-04-04
- Description: Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-04-25

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

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

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

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

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

- OSSINDEX - [CVE-2022-22965] CWE-94: Improper Control of Generation of Code ('Code Injection')
- OSSINDEX - [sonatype-2022-1764] CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
- OSSIndex - http://web.archive.org/web/20220330064100/https://twitter.com/shyest_sys/status/1509053689331335174
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965
- OSSIndex - https://blog.sonatype.com/new-0-day-spring-framework-vulnerability-confirmed-patch-now
- OSSIndex - https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- OSSIndex - https://www.praetorian.com/blog/spring-core-jdk9-rce/
- OSSIndex - https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

Vulnerable Software & Versions: (show all)

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

CVE-2021-22118 suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210713-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22118
- 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-2021-22118] CWE-668: Exposure of Resource to Wrong Sphere
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118

Vulnerable Software & Versions: (show all)

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

CVE-2022-22950 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://tanzu.vmware.com/security/cve-2022-22950
- OSSINDEX - [CVE-2022-22950] CWE-770: Allocation of Resources Without Limits or Throttling
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28145
- OSSIndex - https://spring.io/blog/2022/03/17/spring-framework-6-0-0-m3-and-5-3-17-available-now
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22950

Vulnerable Software & Versions: (show all)

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

CVE-2022-22971 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0003/
- MISC - https://tanzu.vmware.com/security/cve-2022-22971
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.2.0; versions up to (including) 5.2.21

- ...

CVE-2022-22968 suppress

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

CWE-178 Improper Handling of Case Sensitivity

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220602-0004/
- MISC - https://tanzu.vmware.com/security/cve-2022-22968
- N/A - N/A
- OSSINDEX - [CVE-2022-22968] CWE-178: Improper Handling of Case Sensitivity
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28333
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/28334
- OSSIndex - https://spring.io/blog/2022/04/13/spring-framework-data-binding-rules-vulnerability-cve-2022-22968
- OSSIndex - https://tanzu.vmware.com/security/cve-2022-22968

Vulnerable Software & Versions: (show all)

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

CVE-2022-22970 suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220616-0006/
- MISC - https://tanzu.vmware.com/security/cve-2022-22970
- N/A - N/A

Vulnerable Software & Versions: (show all)

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

CVE-2021-22060 suppress

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

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - https://tanzu.vmware.com/security/cve-2021-22060
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22060] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22060

Vulnerable Software & Versions: (show all)

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

CVE-2021-22096 suppress

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

NVD-CWE-Other

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

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20211125-0005/
- MISC - https://tanzu.vmware.com/security/cve-2021-22096
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- OSSINDEX - [CVE-2021-22096] CWE-117: Improper Output Neutralization for Logs
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22096

Vulnerable Software & Versions: (show all)

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

tomcat-embed-core-9.0.38.jar

Description:

Core Tomcat implementation

License:

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

File Path: /Users/djvelickovic/.m2/repository/org/apache/tomcat/embed/tomcat-embed-core/9.0.38/tomcat-embed-core-9.0.38.jar
MD5: f98862daa7adeddd61eaa61c7ad34d45
SHA1: 368aac73f9274896fa8cccf20f4799533629471c
SHA256:e1359b3f399b3e0f9d02839f7ed8104fa4ac2019392a18a929681d2968794d6b
Referenced In Project/Scope: engine:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.3.4.RELEASE

Evidence

Related Dependencies

Identifiers

- pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.38 (*Confidence*:High)
- cpe:2.3:a:apache:tomcat:9.0.38:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.38:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-17527 suppress

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

CWE-200 Information Exposure

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

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

References:
- 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 - [announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [debian-lts-announce] 20201216 [SECURITY] [DLA 2495-1] tomcat8 security update
- MLIST - [guacamole-issues] 20201206 [jira] [Commented] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- MLIST - [guacamole-issues] 20201206 [jira] [Created] (GUACAMOLE-1229) Fix in Dockerhub for latest CVE-2020-17527
- MLIST - [oss-security] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [tomcat-announce] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [tomcat-announce] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [tomcat-dev] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [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
- MLIST - [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
- MLIST - [tomcat-dev] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [tomcat-users] 20201203 [SECURITY] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up

- MLIST - [tomcat-users] 20210119 Re: [SECURITY][CORRECTION] CVE-2020-17527 Apache Tomcat HTTP/2 Request header mix-up
- MLIST - [tomee-commits] 20201207 [jira] [Assigned] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- MLIST - [tomee-commits] 20201207 [jira] [Created] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- MLIST - [tomee-commits] 20210319 [jira] [Updated] (TOMEE-2936) TomEE plus(7.0.9) is affected by CVE-2020-17527(BDSA-2020-3628) vulnerability.
- N/A - N/A

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:apache:tomcat:9.0.38:*:*:*:*:*:*:*
- ...

CVE-2021-25122 suppress

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

CWE-200 Information Exposure

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

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

References:
- 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 - [announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- 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
- MLIST - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- MLIST - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- MLIST - [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
- MLIST - [tomcat-users] 20210301 [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- MLIST - [tomcat-users] 20210305 RE: [SECURITY] CVE-2021-25122 Apache Tomcat h2c request mix-up
- MLIST - [tomcat-users] 20210305 Re: [SECURITY] 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-2021-41079 suppress

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

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

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

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

References:
- 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
- MLIST - [tomcat-dev] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS
- MLIST - [tomcat-users] 20211014 [SECURITY] CVE-2021-42340 Apache Tomcat DoS

Vulnerable Software & Versions: (show all)

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

CVE-2022-29885 suppress

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

CWE-400 Uncontrolled Resource Consumption ('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: CVSS:3.1/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 - 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-2022-42252 suppress

If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

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

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

References:
- MISC - https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq

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-2020-9484 suppress

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

CWE-502 Deserialization of Untrusted Data

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

CVSSv3:
- Base Score: HIGH (7.0)
- Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- CONFIRM - https://security.netapp.com/advisory/ntap-20200528-0005/
- DEBIAN - DSA-4727
- FEDORA - FEDORA-2020-ce396e7d5c
- FEDORA - FEDORA-2020-d9169235a8
- 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 - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- 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
- MLIST - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [tomcat-dev] 20200527 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- MLIST - [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
- MLIST - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [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
- MLIST - [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
- MLIST - [tomcat-users] 20200521 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- MLIST - [tomcat-users] 20200524 Re: [SECURITY] CVE-2020-9484 Apache Tomcat Remote Code Execution via session persistence
- MLIST - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- MLIST - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- MLIST - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- MLIST - [tomee-commits] 20201013 [jira] [Assigned] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- MLIST - [tomee-commits] 20201013 [jira] [Commented] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- MLIST - [tomee-commits] 20201013 [jira] [Created] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- MLIST - [tomee-commits] 20201013 [jira] [Updated] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- MLIST - [tomee-commits] 20210522 [jira] [Closed] (TOMEE-2909) Impact of security vulnerability(CVE-2020-9484) on TOMEE plus (7.0.7)
- 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-2021-25329 suppress

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

NVD-CWE-noinfo

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

CVSSv3:
- Base Score: HIGH (7.0)
- Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- 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 - [announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- 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
- MLIST - [tomcat-announce] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [tomcat-dev] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [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
- MLIST - [tomcat-users] 20210301 [SECURITY] CVE-2021-25329 Apache Tomcat Incomplete fix for CVE-2020-9484 (RCE via session persistence)
- MLIST - [tomcat-users] 20210701 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- MLIST - [tomcat-users] 20210701 What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- MLIST - [tomcat-users] 20210702 Re: CVE-2021-25329, was Re: Most recent security-related update to 8.5
- MLIST - [tomcat-users] 20210702 Re: What is "h2c"? What is CVE-2021-25329? Re: Most recent security-related update to 8.5
- 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-2022-23181 suppress

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

CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

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

CVSSv3:
- Base Score: HIGH (7.0)
- Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20220217-0010/
- DEBIAN - DSA-5265
- MISC - https://lists.apache.org/thread/l8x62p3k19yfcb208jo4zrb83k5mfwg9
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- 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) 9.0.35; versions up to (including) 9.0.56
- ...

CVE-2021-30640 suppress

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

CWE-116 Improper Encoding or Escaping of Output

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

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N

References:
- 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-2022-34305 suppress

In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.

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

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

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

References:
- 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-2021-24122 suppress

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

CWE-706 Use of Incorrectly-Resolved Name or Reference

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

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210212-0008/
- MISC - https://lists.apache.org/thread.html/r1595889b083e05986f42b944dc43060d6b083022260b6ea64d2cec52%40%3Cannounce.tomcat.apache.org%3E
- MLIST - [announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- MLIST - [debian-lts-announce] 20210316 [SECURITY] [DLA 2596-1] tomcat8 security update
- MLIST - [oss-security] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- MLIST - [tomcat-announce] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- MLIST - [tomcat-dev] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- MLIST - [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
- MLIST - [tomcat-users] 20210114 [SECURITY] CVE-2021-24122 Apache Tomcat Information Disclosure
- MLIST - [tomee-dev] 20210114 Re: Releases?
- MLIST - [tomee-dev] 20210115 CVE-2021-24122 NTFS Information Disclosure Bug
- 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-2021-33037 suppress

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

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

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- 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
- MLIST - [tomee-commits] 20210728 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- MLIST - [tomee-commits] 20210728 [jira] [Created] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- MLIST - [tomee-commits] 20210830 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- MLIST - [tomee-commits] 20210913 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- MLIST - [tomee-commits] 20210914 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- MLIST - [tomee-commits] 20210916 [jira] [Resolved] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037
- 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-2021-43980 suppress

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

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

CVSSv3:

- Base Score: LOW (3.7)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

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
- ...

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