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

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

Sponsor

Project: rest-service

com.twk:rest-service:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 8.0.1
- *Report Generated On*: Sat, 21 Jan 2023 13:49:44 -0500
- *Dependencies Scanned*: 38 (22 unique)
- *Vulnerable Dependencies*: 13
- *Vulnerabilities Found*: 101
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs↓	Package	Highest Severity	CVE Coun
spring-boot-starter-web-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:2.2.4:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE	HIGH	1
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	HIGH	1
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	HIGH	8
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	1
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
spring-webmvc-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE	CRITICAL*	9
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	CRITICAL*	10
spring-core-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.2.3.RELEASE	CRITICAL*	9
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	4
bcprov-jdk15on-1.46.jar	cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.46:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.46:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46	HIGH	17
tomcat-embed-websocket-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30	CRITICAL*	20
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL*	19
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1

* indicates the dependency has a known exploited vulnerability

Dependencies

bcprov-jdk15on-1.46.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 1.7.

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\bouncycastle\bcprov-jdk15on\1.46\bcprov-jdk15on-1.46.jar
MD5: b94e6fef30e871f1b4117232cdc75369
SHA1: 991c96a4e31e6c19e2b9136c8955bd423f2dc4c7
SHA256:a1952237d941ef0b6122ba27b0b58de602de91c714ba3ddd4eef30ba3f5a0a67
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/com.twk/rest-service@0.0.1-SNAPSHOT

Evidence

Identifiers

- pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46 (*Confidence*:High)
- cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.46:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.46:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2016-1000338 suppress

In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.

CWE-347 Improper Verification of Cryptographic Signature

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

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/b0c3ce99d43d73a096268831d0d120ffc89eac7f#diff-3679f5a9d2b939d0d3ee1601a7774fb0
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- MLIST - [lucene-solr-user] 20190104 Re: SOLR v7 Security Issues Caused Denial of Use - Sonatype Application Composition Report
- OSSINDEX - [CVE-2016-1000338] CWE-347: Improper Verification of Cryptographic Signature
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000338
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000342 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier ECDSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.

CWE-347 Improper Verification of Cryptographic Signature

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

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/843c2e60f67d71faf81d236f448ebbe56c62c647#diff-25c3c78db788365f36839b3f2d3016b9
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- OSSINDEX - [CVE-2016-1000342] CWE-347: Improper Verification of Cryptographic Signature
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000342
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000343 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the DSA key pair generator generates a weak private key if used with default values. If the JCA key pair generator is not explicitly initialised with DSA parameters, 1.55 and earlier generates a private value assuming a 1024 bit key size. In earlier releases this can be dealt with by explicitly passing parameters to the key pair generator.

CWE-310 Cryptographic Issues

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

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/50a53068c094d6cff37659da33c9b4505becd389#diff-5578e61500abb2b87b300d3114bdfd7d
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- MLIST - [lucene-solr-user] 20190104 Re: SOLR v7 Security Issues Caused Denial of Use - Sonatype Application Composition Report
- OSSINDEX - [CVE-2016-1000343] CWE-310
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000343
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000344 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

CWE-310 Cryptographic Issues

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

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/9385b0ebd277724b167fe1d1456e3c112112be1f
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000352 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

CWE-310 Cryptographic Issues

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

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/9385b0ebd277724b167fe1d1456e3c112112be1f
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000341 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier DSA signature generation is vulnerable to timing attack. Where timings can be closely observed for the generation of signatures, the lack of blinding in 1.55, or earlier, may allow an attacker to gain information about the signature's k value and ultimately the private value as well.

CWE-361 7PK - Time and State

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

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/acaac81f96fec91ab45bd0412beaf9c3acd8defa#diff-e75226a9ca49217a7276b29242ec59ce
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- OSSINDEX - [CVE-2016-1000341] CWE-361
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000341
- OSSIndex - https://rdist.root.org/2010/11/19/dsa-requirements-for-random-k-value/
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2016-1000345 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES/ECIES CBC mode vulnerable to padding oracle attack. For BC 1.55 and older, in an environment where timings can be easily observed, it is possible with enough observations to identify when the decryption is failing due to padding.

CWE-361 7PK - Time and State

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

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/21dcb3d9744c83dcf2ff8fcee06dbca7bfa4ef35#diff-4439ce586bf9a13bfec05c0d113b8098
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- OSSINDEX - [CVE-2016-1000345] CWE-361
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000345
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2017-13098 suppress

BouncyCastle TLS prior to version 1.0.3, when configured to use the JCE (Java Cryptography Extension) for cryptographic functions, provides a weak Bleichenbacher oracle when any TLS cipher suite using RSA key exchange is negotiated. An attacker can recover the private key from a vulnerable application. This vulnerability is referred to as "ROBOT."

CWE-203 Information Exposure Through Discrepancy

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

References:
- BID - 102195
- CERT-VN - VU#144389
- CONFIRM - https://github.com/bcgit/bc-java/commit/a00b684465b38d722ca9a3543b8af8568e6bad5c
- CONFIRM - https://security.netapp.com/advisory/ntap-20171222-0001/
- DEBIAN - DSA-4072
- MISC - https://robotattack.org/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- SUSE - openSUSE-SU-2020:0607

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (excluding) 1.59

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:1.46:*:*:*:*:*:*:*

CVE-2016-1000339 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the primary engine class used for AES was AESFastEngine. Due to the highly table driven approach used in the algorithm it turns out that if the data channel on the CPU can be monitored the lookup table accesses are sufficient to leak information on the AES key being used. There was also a leak in AESEngine although it was substantially less. AESEngine has been modified to remove any signs of leakage (testing carried out on Intel X86-64) and is now the primary AES class for the BC JCE provider from 1.56. Use of AESFastEngine is now only recommended where otherwise deemed appropriate.

CWE-310 Cryptographic Issues

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

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/413b42f4d770456508585c830cfcde95f9b0e93b#diff-54656f860db94b867ba7542430cd2ef0
- CONFIRM - https://github.com/bcgit/bc-java/commit/8a73f08931450c17c749af067b6a8185abdfd2c0#diff-494fb066bed02aeb76b6c005632943f2
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2020-26939 (OSSINDEX) suppress

In Legion of the Bouncy Castle BC before 1.61 and BC-FJA before 1.0.1.2, attackers can obtain sensitive information about a private exponent because of Observable Differences in Behavior to Error Inputs. This occurs in org.bouncycastle.crypto.encodings.OAEPEncoding. Sending invalid ciphertext that decrypts to a short payload in the OAEP Decoder could result in the throwing of an early exception, potentially leaking some information about the private exponent of the RSA private key performing the encryption.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2020-26939 for details

CWE-203 Information Exposure Through Discrepancy

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

References:
- OSSINDEX - [CVE-2020-26939] CWE-203: Information Exposure Through Discrepancy
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-26939
- OSSIndex - https://github.com/bcgit/bc-java/wiki/CVE-2020-26939

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:*:*:*:*:*:*:*

CVE-2015-7940 suppress

The Bouncy Castle Java library before 1.51 does not validate a point is withing the elliptic curve, which makes it easier for remote attackers to obtain private keys via a series of crafted elliptic curve Diffie Hellman (ECDH) key exchanges, aka an "invalid curve attack."

CWE-310 Cryptographic Issues, CWE-200 Information Exposure

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

References:

- BID - 79091
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
- CONFIRM - http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM - https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
- DEBIAN - DSA-3417
- FEDORA - FEDORA-2015-7d95466eda
- MISC - http://web-in-security.blogspot.ca/2015/09/practical-invalid-curve-attacks.html
- MLIST - [oss-security] 20151022 CVE Request: invalid curve attack on bouncycastle
- MLIST - [oss-security] 20151022 Re: CVE Request: invalid curve attack on bouncycastle
- N/A - N/A
- OSSINDEX - [CVE-2015-7940] CWE-200: Information Exposure
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7940
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=1276272
- REDHAT - RHSA-2016:2035
- REDHAT - RHSA-2016:2036
- SECTRACK - 1037036
- SECTRACK - 1037046
- SECTRACK - 1037053
- SUSE - openSUSE-SU-2015:1911
- UBUNTU - USN-3727-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:*:*:*:*:*:*:*:* versions up to (including) 1.50
- ...

CVE-2018-5382 suppress

The default BKS keystore use an HMAC that is only 16 bits long, which can allow an attacker to compromise the integrity of a BKS keystore. Bouncy Castle release 1.47 changes the BKS format to a format which uses a 160 bit HMAC instead. This applies to any BKS keystore generated prior to BC 1.47. For situations where people need to create the files for legacy reasons a specific keystore type "BKS-V1" was introduced in 1.49. It should be noted that the use of "BKS-V1" is discouraged by the library authors and should only be used where it is otherwise safe to do so, as in where the use of a 16 bit checksum for the file integrity check is not going to cause a security issue in itself.

CWE-354 Improper Validation of Integrity Check Value

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.4)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- BID - 103453
- CERT-VN - VU#306792
- MISC - https://www.bouncycastle.org/releasenotes.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- OSSINDEX - [CVE-2018-5382] CWE-354: Improper Validation of Integrity Check Value
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5382
- OSSIndex - https://blog.sonatype.com/cve-2018-2018-5382-bouncycastle-information-exposure
- OSSIndex - https://insights.sei.cmu.edu/cert/2018/03/the-curious-case-of-the-bouncy-castle-bks-passwords.html
- OSSIndex - https://www.bouncycastle.org/releasenotes.html
- OSSIndex - https://www.kb.cert.org/vuls/id/306792
- REDHAT - RHSA-2018:2927

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.49
- ...

CVE-2013-1624 suppress

The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

CWE-310 Cryptographic Issues

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

References:
- MISC - http://www.isg.rhul.ac.uk/tls/TLStiming.pdf
- MLIST - [oss-security] 20130205 Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations
- OSSINDEX - [CVE-2013-1624] CWE-310
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=908428
- REDHAT - RHSA-2014:0371
- REDHAT - RHSA-2014:0372
- SECUNIA - 57716
- SECUNIA - 57719

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:*:*:*:*:*:*:*
- ...

CVE-2016-1000346 suppress

In the Bouncy Castle JCE Provider version 1.55 and earlier the other party DH public key is not fully validated. This can cause issues as invalid keys can be used to reveal details about the other party's private key where static Diffie-Hellman is in use. As of release 1.56 the key parameters are checked on agreement calculation.

CWE-320 Key Management Errors

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

CVSSv3:
- Base Score: LOW (3.7)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://github.com/bcgit/bc-java/commit/1127131c89021612c6eefa26dbe5714c194e7495#diff-d525a20b8acaed791ae2f0f770eb5937
- CONFIRM - https://security.netapp.com/advisory/ntap-20181127-0004/
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20180707 [SECURITY] [DLA 1418-1] bouncycastle security update
- OSSINDEX - [CVE-2016-1000346] CWE-320
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000346
- OSSIndex - https://news.ycombinator.com/item?id=7959519
- REDHAT - RHSA-2018:2669
- REDHAT - RHSA-2018:2927
- UBUNTU - USN-3727-1

Vulnerable Software & Versions:

- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:*:*:*:*:*:*:*:* versions up to (including) 1.55

CVE-2015-6644 (OSSINDEX) suppress

Bouncy Castle in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information via a crafted application, aka internal bug 24106146.

CWE-200 Information Exposure

CVSSv3:
- Base Score: LOW (3.3)
- Vector: CVSS:/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

References:
- OSSINDEX - [CVE-2015-6644] CWE-200: Information Exposure
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6644
- OSSIndex - https://bugzilla.redhat.com/show_bug.cgi?id=1444015
- OSSIndex - https://github.com/bcgit/bc-java/issues/177

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.46:*:*:*:*:*:*:*

hibernate-validator-6.0.18.Final.jar

Description:

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

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\hibernate\validator\hibernate-validator\6.0.18.Final\hibernate-validator-6.0.18.Final.jar
MD5: d3eeb4f1bf013d939b86dfc34b0c6a5d
SHA1: 7fd00bcd87e14b6ba66279282ef15efa30dd2492
SHA256:79fb11445bc48e1ea6fb259e825d58b3c9a5fa2b7e3c9527e41e4aeda82de907
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-10693 suppress

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

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I: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://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MLIST - [portals-pluto-dev] 20210714 [jira] [Closed] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- MLIST - [portals-pluto-dev] 20210714 [jira] [Created] (PLUTO-791) Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- MLIST - [portals-pluto-scm] 20210714 [portals-pluto] branch master updated: PLUTO-791 Upgrade to hibernate-validator-6.0.20.Final due to CVE-2020-10693 and CVE-2019-10219
- OSSINDEX - [CVE-2020-10693] CWE-20: Improper Input Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693
- OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1092
- OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1093
- OSSIndex - https://github.com/hibernate/hibernate-validator/pull/1094
- OSSIndex - https://hibernate.atlassian.net/browse/HV-1774
- OSSIndex - https://in.relation.to/2020/05/07/hibernate-validator-615-6020-released/
- OSSIndex - https://openliberty.io/docs/latest/security-vulnerabilities.html

Vulnerable Software & Versions: (show all)

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

jackson-databind-2.10.2.jar

Description:

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

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\com\fasterxml\jackson\core\jackson-databind\2.10.2\jackson-databind-2.10.2.jar
MD5: 057751b4e2dd1104be8caad6e9a3e589
SHA1: 0528de95f198afafbcfb0c09d2e43b6e0ea663ec
SHA256:42c25644e35fadfbded1b7f35a8d1e70a86737f190e43aa2c56cea4b96cbda88
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-25649 suppress

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

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

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210108-0007/
- FEDORA - FEDORA-2021-1d8254899c
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1887664
- MISC - https://github.com/FasterXML/jackson-databind/issues/2589
- MISC - https://lists.apache.org/thread.html/r31f4ee7d561d56a0c2c2c6eb1d6ce3e05917ff9654fdbfec05dc2b83@%3Ccommits.servicecomb.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 - [druid-commits] 20201208 [GitHub] [druid] jihoonson opened a new pull request #10655: Bump up jackson-databind to 2.10.5.1
- MLIST - [flink-issues] 20210121 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- MLIST - [flink-issues] 20210122 [GitHub] [flink-shaded] HuangXingBo opened a new pull request #93: [FLINK-21020][jackson] Bump version to 2.12.1
- MLIST - [hive-dev] 20210223 [jira] [Created] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210223 [jira] [Assigned] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210223 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649

- MLIST - [hive-issues] 20210223 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210315 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210316 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210503 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210510 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20210514 [jira] [Work logged] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20211012 [jira] [Resolved] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [hive-issues] 20211012 [jira] [Updated] (HIVE-24816) Upgrade jackson to 2.10.5.1 or 2.11.0+ due to CVE-2020-25649
- MLIST - [iotdb-commits] 20210325 [iotdb] branch master updated: [IOTDB-1256] upgrade Jackson to 2.11.0 because of loopholes CVE-2020-25649 (#2896)
- MLIST - [iotdb-notifications] 20210324 [jira] [Created] (IOTDB-1256) Jackson have loopholes CVE-2020-25649
- MLIST - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 closed pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- MLIST - [iotdb-reviews] 20210324 [GitHub] [iotdb] wangchao316 opened a new pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- MLIST - [iotdb-reviews] 20210325 [GitHub] [iotdb] jixuan1989 merged pull request #2896: [IOTDB-1256] Jackson have loopholes CVE-2020-25649
- MLIST - [kafka-dev] 20201215 Re: [VOTE] 2.7.0 RC5
- MLIST - [kafka-dev] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- MLIST - [kafka-dev] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- MLIST - [kafka-dev] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- MLIST - [kafka-jira] 20201205 [GitHub] [kafka] sirocchj opened a new pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201209 [GitHub] [kafka] jjuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201209 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201209 [GitHub] [kafka] sirocchj edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201210 [GitHub] [kafka] niteshmor edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201210 [GitHub] [kafka] sirocchj commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201215 [GitHub] [kafka] jjuma commented on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201215 [GitHub] [kafka] jjuma edited a comment on pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-jira] 20201215 [GitHub] [kafka] jjuma merged pull request #9702: CVE-2020-25649: bumping jackson to patched version 2.10.5.1
- MLIST - [kafka-users] 20201215 Re: [VOTE] 2.7.0 RC5
- MLIST - [kafka-users] 20210105 Re: [kafka-clients] Re: [VOTE] 2.6.1 RC3
- MLIST - [kafka-users] 20210831 Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- MLIST - [kafka-users] 20210901 Re: [EXTERNAL] Re: Security vulnerabilities in kafka:2.13-2.6.0/2.7.0 docker image
- MLIST - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre commented on pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- MLIST - [karaf-commits] 20210217 [GitHub] [karaf] jbonofre merged pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- MLIST - [karaf-commits] 20210217 [GitHub] [karaf] svogt opened a new pull request #1296: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- MLIST - [karaf-commits] 20210217 [karaf] branch master updated: Update jackson-databind to fix CVE-2020-25649 / BDSA-2020-2965
- MLIST - [knox-dev] 20210601 [jira] [Created] (KNOX-2614) Upgrade Jackson due to CVE-2020-25649
- MLIST - [knox-dev] 20210601 [jira] [Updated] (KNOX-2614) Upgrade jackson-databind to 2.10.5 due to CVE-2020-25649
- MLIST - [spark-user] 20210621 Re: CVEs
- MLIST - [tomee-commits] 20210127 [jira] [Created] (TOMEE-2965) CVE-2020-25649 - Update jackson databind
- MLIST - [turbine-commits] 20210316 svn commit: r1887732 - in /turbine/fulcrum/trunk/json: ./ jackson/ jackson/src/test/org/apache/fulcrum/json/jackson/ jackson2/ jackson2/src/test/org/apache/fulcrum/json/jackson/ jackson2/src/test/org/apache/fulcrum/json/jackson/mixins/
- MLIST - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.5.9 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-commits] 20210106 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-commits] 20210106 [zookeeper] branch master updated: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-dev] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-issues] 20210105 [jira] [Created] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-issues] 20210105 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-issues] 20210106 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-issues] 20210106 [jira] [Updated] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-issues] 20210116 [jira] [Commented] (ZOOKEEPER-4045) CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] asfgit closed pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] edwin092 opened a new pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- MLIST - [zookeeper-notifications] 20210106 [GitHub] [zookeeper] nkalmar commented on pull request #1572: ZOOKEEPER-4045: CVE-2020-25649 - Upgrade jackson databind to 2.10.5.1
- N/A - N/A
- N/A - N/A
- OSSINDEX - [CVE-2020-25649] CWE-611: Improper Restriction of XML External Entity Reference ('XXE')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649
- OSSIndex - https://github.com/FasterXML/jackson-databind/issues/2589

Vulnerable Software & Versions: (show all)

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

CVE-2020-36518 suppress

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

CWE-787 Out-of-bounds Write

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

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

References:
- 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
- ...

log4j-api-2.12.1.jar

Description:

The Apache Log4j API

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\apache\logging\log4j\log4j-api\2.12.1\log4j-api-2.12.1.jar
MD5: 4a6f276d4fb426c8d489343c0325bb75
SHA1: a55e6d987f50a515c9260b0451b4fa217dc539cb
SHA256:429534d03bdb728879ab551d469e26f6f7ff4c8a8627f59ac68ab6ef26063515
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-9488 suppress

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

CWE-295 Improper Certificate Validation

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

CVSSv3:
- Base Score: LOW (3.7)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

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

Vulnerable Software & Versions: (show all)

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

logback-core-1.2.3.jar

Description:

logback-core module

License:

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

File Path: C:\Users\Kyle Dale\.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: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.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
- ...

snakeyaml-1.25.jar

Description:

YAML 1.1 parser and emitter for Java

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\yaml\snakeyaml\1.25\snakeyaml-1.25.jar
MD5: 6f7d5b8f596047aae07a3bf6f23a0bf2
SHA1: 8b6e01ef661d8378ae6dd7b511a7f2a33fae1421
SHA256:b50ef33187e7dc922b26dbe4dd0fdb3a9cf349e75a08b95269901548eee546eb
Referenced In Project/Scope: rest-service:runtime
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-1471 (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:1.25:*:*:*:*:*:*:*

CVE-2017-18640 suppress

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

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

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

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

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

- OSSINDEX - [CVE-2017-18640] CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640
- OSSIndex - https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion

Vulnerable Software & Versions: (show all)

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

CVE-2022-25857 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-2.2.4.RELEASE.jar

Description:

Spring Boot

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\springframework\boot\spring-boot\2.2.4.RELEASE\spring-boot-2.2.4.RELEASE.jar
MD5: 24de0cfd8ea74b903b562b43cbc5eb13
SHA1: 225a4fd31156c254e3bb92adb42ee8c6de812714
SHA256:176befc7b90e8498f44e21994a70d69ba360ef1e858ff3cea8282e802372daf2
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Related Dependencies

Identifiers

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

Published Vulnerabilities

CVE-2022-27772 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.

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:
- MISC - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- OSSINDEX - [CVE-2022-27772] CWE-668: Exposure of Resource to Wrong Sphere
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772
- OSSIndex - https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85
- OSSIndex - https://github.com/github/codeql/pull/4473#issuecomment-1030416237
- OSSIndex - https://github.com/spring-projects/spring-boot/issues/23622

Vulnerable Software & Versions:

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

spring-boot-starter-web-2.2.4.RELEASE.jar

Description:

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

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\springframework\boot\spring-boot-starter-web\2.2.4.RELEASE\spring-boot-starter-web-2.2.4.RELEASE.jar
MD5: 0fd2927b6235bdbaa0d4d12c28a847c2
SHA1: ec75d01d212b5229c16d872fb127744c0ed46ed8
SHA256:eb4d4ad19fe1724fd02cfce9c467c0b67766b5a4a54d0e54fc51826d9e3d87b8
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/com.twk/rest-service@0.0.1-SNAPSHOT

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-27772 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.

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

Vulnerable Software & Versions:

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

spring-core-5.2.3.RELEASE.jar

Description:

Spring Core

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\springframework\spring-core\5.2.3.RELEASE\spring-core-5.2.3.RELEASE.jar
MD5: ae11e44d9eff630186b9e095e70b59de
SHA1: 3734223040040e8c3fecd5faa3ae8a1ed6da146b
SHA256:6df908f4deaeefd2b03b56a00246cc0dc0d941d9636e811025bc6fc5a2a44851
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-test@2.2.4.RELEASE

Evidence

Related Dependencies

Identifiers

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

Published Vulnerabilities

CVE-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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-5421 suppress

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

NVD-CWE-noinfo

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210513-0009/
- CONFIRM - https://tanzu.vmware.com/security/cve-2020-5421
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [ignite-user] 20201117 Query on CVE-2020-5421
- MLIST - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- MLIST - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- 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 (excluding) 5.2.9
- ...

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

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

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

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

Vulnerable Software & Versions: (show all)

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

spring-web-5.2.3.RELEASE.jar

Description:

Spring Web

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\springframework\spring-web\5.2.3.RELEASE\spring-web-5.2.3.RELEASE.jar
MD5: a89d66690cd14159aa6ac1e875e54411
SHA1: dd386a02e40b915ab400a3bf9f586d2dc4c0852c
SHA256:25d264969c624cb8103a7f2b36b148ea1be8b87780c4758e7f9a6e2bc8416d76
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2016-1000027 suppress

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

CWE-502 Deserialization of Untrusted Data

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

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-2020-5421 suppress

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

NVD-CWE-noinfo

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210513-0009/
- CONFIRM - https://tanzu.vmware.com/security/cve-2020-5421
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421

- MLIST - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [ignite-user] 20201117 Query on CVE-2020-5421
- MLIST - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- MLIST - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- N/A - N/A
- OSSINDEX - [CVE-2020-5421] CWE-20: Improper Input Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421
- OSSIndex - https://tanzu.vmware.com/security/cve-2020-5421

Vulnerable Software & Versions: (show all)

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

CVE-2022-22950 suppress

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

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

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

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-5.2.3.RELEASE.jar

Description:

Spring Web MVC

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\springframework\spring-webmvc\5.2.3.RELEASE\spring-webmvc-5.2.3.RELEASE.jar
MD5: 867cc7369d453637b5042ee4d6931a78
SHA1: 745a62502023d2496b565b7fe102bb1ee229d6b7
SHA256:b3b0a2477e67b050dd5c08dc96e76db5950cbccba075e782c24f73eda49a0160

Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2022-22965 suppress

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-5421 suppress

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

NVD-CWE-noinfo

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:N/AC:H/Au:S/C:P/I:P/A:N

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20210513-0009/
- CONFIRM - https://tanzu.vmware.com/security/cve-2020-5421
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko opened a new pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- MLIST - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- MLIST - [ignite-user] 20201117 Query on CVE-2020-5421
- MLIST - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- MLIST - [pulsar-commits] 20201022 [GitHub] [pulsar] Ghatage opened a new pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- MLIST - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- 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 (excluding) 5.2.9
- ...

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

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

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

Vulnerable Software & Versions: (show all)

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

- ...

tomcat-embed-core-9.0.30.jar

Description:

Core Tomcat implementation

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\apache\tomcat\embed\tomcat-embed-core\9.0.30\tomcat-embed-core-9.0.30.jar
MD5: f9e49f66756f133157f19e617af26ffe
SHA1: ad32909314fe2ba02cec036434c0addd19bcc580
SHA256:b1415eecbc9f14e3745c1bfd41512a1b8e1af1332a7beaed4be30b2e0ba7b330
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-1938 suppress

CISA Known Exploited Vulnerability:

- Product: Apache Tomcat
- Name: Apache Tomcat Improper Privilege Management Vulnerability
- Date Added: 2022-03-03
- Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-03-17

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

NVD-CWE-Other

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

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

References:
- CONFIRM - http://support.blackberry.com/kb/articleDetail?articleNumber=000062739
- CONFIRM - https://security.netapp.com/advisory/ntap-20200226-0002/
- DEBIAN - DSA-4673
- DEBIAN - DSA-4680
- FEDORA - FEDORA-2020-04ac174fa9
- FEDORA - FEDORA-2020-0e42878ba7
- FEDORA - FEDORA-2020-c870aa8378
- GENTOO - GLSA-202003-43
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [announce] 20210125 Apache Software Foundation Security Report: 2020
- MLIST - [announce] 20210223 Re: Apache Software Foundation Security Report: 2020
- MLIST - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- MLIST - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- MLIST - [httpd-bugs] 20200319 [Bug 53098] mod_proxy_ajp: patch to set worker secret passed to tomcat
- MLIST - [ofbiz-commits] 20200227 [ofbiz-plugins] branch release17.12 updated: Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938) (OFBIZ-11407)
- MLIST - [ofbiz-notifications] 20200225 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200225 [jira] [Updated] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200227 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)

- MLIST - [ofbiz-notifications] 20200228 [jira] [Comment Edited] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200228 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-dev] 20200304 Re: Tagging 10.0.x, 9.0.x, 8.5.x
- MLIST - [tomcat-dev] 20200309 [Bug 64206] Answer file not being used
- 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-users] 20200301 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-users] 20200302 AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- MLIST - [tomcat-users] 20200302 Re: AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- MLIST - [tomcat-users] 20200302 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-users] 20200304 Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200305 Aw: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200305 Re: Aw: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200309 Re: Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check)
- MLIST - [tomcat-users] 20200310 Aw: Re: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200310 Re: Re: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200413 RE: Alternatives for AJP
- MLIST - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2789) TomEE plus is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20200320 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20201127 [jira] [Resolved] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20201127 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-dev] 20200311 CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- MLIST - [tomee-dev] 20200311 Re: CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- MLIST - [tomee-dev] 20200316 RE: CVE-2020-8840 on TomEE 8.0.1
- MLIST - [tomee-users] 20200723 Re: TomEE on Docker
- SUSE - openSUSE-SU-2020:0345
- SUSE - openSUSE-SU-2020:0597

Vulnerable Software & Versions: (show all)

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

CVE-2020-11996 suppress

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

NVD-CWE-noinfo

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-13934 suppress

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

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

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

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: 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-20200724-0003/
- DEBIAN - DSA-4727
- MISC - https://lists.apache.org/thread.html/r61f411cf82488d6ec213063fc15feeeb88e31b0ca9c29652ee4f962e%40%3Cannounce.tomcat.apache.org%3E
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- MLIST - [tomcat-dev] 20200818 [Bug 64671] HTTP/2 Stream.receivedData method throwing continuous NullPointerException in the logs
- N/A - N/A
- SUSE - openSUSE-SU-2020:1102
- SUSE - openSUSE-SU-2020:1111
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

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

CVE-2020-13935 suppress

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

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

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

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

References:
- CONFIRM - https://kc.mcafee.com/corporate/index?page=content&id=SB10332
- CONFIRM - https://security.netapp.com/advisory/ntap-20200724-0003/
- DEBIAN - DSA-4727
- MISC - https://lists.apache.org/thread.html/rd48c72bd3255bda87564d4da3791517c074d94f8a701f93b857526 51%40%3Cannounce.tomcat.apache.org%3E
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpuapr2022.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2021.html
- MLIST - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- MLIST - [tomcat-users] 20201118 Re: Strange crash-on-takeoff, Tomcat 7.0.104
- N/A - N/A
- SUSE - openSUSE-SU-2020:1102
- SUSE - openSUSE-SU-2020:1111
- UBUNTU - USN-4448-1
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

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

CVE-2020-17527 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:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.35
- ...

CVE-2021-25122 suppress

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

CWE-200 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-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-2019-17569 suppress

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

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

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

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

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20200327-0005/
- DEBIAN - DSA-4673
- DEBIAN - DSA-4680
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update

- MLIST - [tomcat-announce] 20200224 [SECURITY] CVE-2019-17569 HTTP Request Smuggling
- MLIST - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- MLIST - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2790) TomEE plus(7.0.7) is affected by CVE-2020-1935 & CVE-2019-17569 vulnerabilities
- SUSE - openSUSE-SU-2020:0345

Vulnerable Software & Versions: (show all)

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

CVE-2020-1935 suppress

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

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

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-13943 suppress

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

NVD-CWE-noinfo

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-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
- ...

tomcat-embed-websocket-9.0.30.jar

Description:

Core Tomcat implementation

License:

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

File Path: C:\Users\Kyle Dale\.m2\repository\org\apache\tomcat\embed\tomcat-embed-websocket\9.0.30\tomcat-embed-websocket-9.0.30.jar
MD5: 3b6e5bcc92cd9a6df4a17138ed4e011c
SHA1: 33157f6bc5bfd03380ebb5ac476db0600a04168d
SHA256:4ce32add19b34a80376edb1e1678c373cb720c28c7a0d37a4361bf659c2ea84c
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE

Evidence

Identifiers

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

Published Vulnerabilities

CVE-2020-1938 suppress

CISA Known Exploited Vulnerability:

- Product: Apache Tomcat
- Name: Apache Tomcat Improper Privilege Management Vulnerability
- Date Added: 2022-03-03
- Description: Apache Tomcat treats Apache JServ Protocol (AJP) connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited.
- Required Action: Apply updates per vendor instructions.
- Due Date: 2022-03-17

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

NVD-CWE-Other

CVSSv2:

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

CVSSv3:

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

References:

- CONFIRM - http://support.blackberry.com/kb/articleDetail?articleNumber=000062739
- CONFIRM - https://security.netapp.com/advisory/ntap-20200226-0002/
- DEBIAN - DSA-4673
- DEBIAN - DSA-4680
- FEDORA - FEDORA-2020-04ac174fa9
- FEDORA - FEDORA-2020-0e42878ba7
- FEDORA - FEDORA-2020-c870aa8378
- GENTOO - GLSA-202003-43
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujul2020.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [announce] 20210125 Apache Software Foundation Security Report: 2020
- MLIST - [announce] 20210223 Re: Apache Software Foundation Security Report: 2020
- MLIST - [debian-lts-announce] 20200304 [SECURITY] [DLA 2133-1] tomcat7 security update
- MLIST - [debian-lts-announce] 20200528 [SECURITY] [DLA 2209-1] tomcat8 security update
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- MLIST - [httpd-bugs] 20200319 [Bug 53098] mod_proxy_ajp: patch to set worker secret passed to tomcat

- MLIST - [ofbiz-commits] 20200227 [ofbiz-plugins] branch release17.12 updated: Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938) (OFBIZ-11407)
- MLIST - [ofbiz-notifications] 20200225 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200225 [jira] [Updated] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200227 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200228 [jira] [Comment Edited] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200228 [jira] [Commented] (OFBIZ-11407) Upgrade Tomcat from 9.0.29 to 9.0.31 (CVE-2020-1938)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [tomcat-announce] 20200224 [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-dev] 20200304 Re: Tagging 10.0.x, 9.0.x, 8.5.x
- MLIST - [tomcat-dev] 20200309 [Bug 64206] Answer file not being used
- 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-users] 20200301 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-users] 20200302 AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- MLIST - [tomcat-users] 20200302 Re: AW: [SECURITY] CVE-2020-1938 AJP Request Injection and potentialRemote Code Execution
- MLIST - [tomcat-users] 20200302 Re: [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
- MLIST - [tomcat-users] 20200304 Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200305 Aw: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200305 Re: Aw: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200309 Re: Apache Tomcat AJP File Inclusion Vulnerability (unauthenticated check)
- MLIST - [tomcat-users] 20200310 Aw: Re: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200310 Re: Re: Re: Fix for CVE-2020-1938
- MLIST - [tomcat-users] 20200413 RE: Alternatives for AJP
- MLIST - [tomee-commits] 20200320 [jira] [Created] (TOMEE-2789) TomEE plus is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20200320 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20200323 [jira] [Commented] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20201127 [jira] [Resolved] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-commits] 20201127 [jira] [Updated] (TOMEE-2789) TomEE plus(7.0.7) is affected by CVE-2020-1938(BDSA-2020-0339) vulnerability.
- MLIST - [tomee-dev] 20200311 CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- MLIST - [tomee-dev] 20200311 Re: CVE-2020-1938 on Tomcat 9.0.30 / TomEE 8.0.1
- MLIST - [tomee-dev] 20200316 RE: CVE-2020-8840 on TomEE 8.0.1
- MLIST - [tomee-users] 20200723 Re: TomEE on Docker
- SUSE - openSUSE-SU-2020:0345
- SUSE - openSUSE-SU-2020:0597

Vulnerable Software & Versions: (show all)

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

CVE-2020-8022 suppress

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

CWE-276 Incorrect Default Permissions

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-11996 suppress

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

NVD-CWE-noinfo

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

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

References:
- CONFIRM - https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E
- CONFIRM - https://security.netapp.com/advisory/ntap-20200709-0002/
- DEBIAN - DSA-4727

- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200712 [SECURITY] [DLA 2279-1] tomcat8 security update
- MLIST - [ofbiz-commits] 20200628 [ofbiz-framework] branch release17.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- MLIST - [ofbiz-commits] 20200628 [ofbiz-framework] branch release18.12 updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- MLIST - [ofbiz-commits] 20200628 [ofbiz-framework] branch trunk updated: Fixed: Upgrades Tomcat to 9.0.36 due to CVE-2020-11996 (OFBIZ-11848)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Created] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200628 [jira] [Updated] (OFBIZ-11847) CLONE - Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200701 [jira] [Reopened] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200703 [jira] [Closed] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200703 [jira] [Comment Edited] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20200703 [jira] [Commented] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [ofbiz-notifications] 20210301 [jira] [Updated] (OFBIZ-11848) Upgrade Tomcat from 9.0.34 to 9.0.36 (CVE-2020-11996)
- MLIST - [tomcat-users] 20201008 Is Tomcat7 supports HTTP2
- SUSE - openSUSE-SU-2020:1051
- SUSE - openSUSE-SU-2020:1063
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

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

CVE-2020-13934 suppress

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

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

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

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: 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-20200724-0003/
- DEBIAN - DSA-4727
- MISC - https://lists.apache.org/thread.html/r61f411cf82488d6ec213063fc15feeeb88e31b0ca9c29652ee4f962e%40%3Cannounce.tomcat.apache.org%3E
- MISC - https://www.oracle.com/security-alerts/cpuApr2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2021.html
- MISC - https://www.oracle.com/security-alerts/cpujan2022.html
- MISC - https://www.oracle.com/security-alerts/cpuoct2020.html
- MLIST - [debian-lts-announce] 20200722 [SECURITY] [DLA 2286-1] tomcat8 security update
- MLIST - [tomcat-dev] 20200818 [Bug 64671] HTTP/2 Stream.receivedData method throwing continuous NullPointerException in the logs
- N/A - N/A
- SUSE - openSUSE-SU-2020:1102
- SUSE - openSUSE-SU-2020:1111
- UBUNTU - USN-4596-1

Vulnerable Software & Versions: (show all)

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

CVE-2020-13935 suppress

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

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

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

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

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

Vulnerable Software & Versions: (show all)

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

- ...

CVE-2020-17527 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:*:*:*:*:*:*:*:* versions from (including) 9.0.1; versions up to (including) 9.0.35
- ...

CVE-2021-25122 suppress

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

CWE-200 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-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-2019-17569 suppress

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

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

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-1935 suppress

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

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

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-2020-13943 suppress

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

NVD-CWE-noinfo

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

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

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

Vulnerable Software & Versions: (show all)

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

CVE-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.