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

Sponsor

Project: rest-service

com.snhu:rest-service:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 12.1.0
- *Report Generated On*: Sun, 17 Aug 2025 18:07:27 -0400
- *Dependencies Scanned*: 48 (26 unique)
- *Vulnerable Dependencies*: 2
- *Vulnerabilities Found*: 6
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidenc
bcprov-jdk15on-1.70.jar	cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_for_java:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.70:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.70	HIGH	5	Highest
spring-core-6.2.9.jar	cpe:2.3:a:pivotal_software:spring_framework:6.2.9:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:6.2.9:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:6.2.9:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@6.2.9	HIGH	1	Highest

Dependencies (vulnerable)

bcprov-jdk15on-1.70.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 and up.

License:

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

File Path: C:\Users\eemar\.m2\repository\org\bouncycastle\bcprov-jdk15on\1.70\bcprov-jdk15on-1.70.jar
MD5: 1809d0449a6374279c01fdd3be26cd92
SHA1: 4636a0d01f74acaf28082fb62b317f1080118371
SHA256:8f3c20e3e2d565d26f33e8d4857a37d0d7f8ac39b62a7026496fcab1bdac30d4
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/com.snhu/rest-service@0.0.1-SNAPSHOT

Evidence

Identifiers

- pkg:maven/org.bouncycastle/bcprov-jdk15on@1.70 (*Confidence*:High)
- cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.70:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.70:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:1.70:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.70:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.70:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2024-34447 (OSSINDEX) suppress

bouncycastle - Improper Validation of Certificate with Host Mismatch

The software communicates with a host that provides a certificate, but the software does not properly ensure that the certificate is actually associated with that host.

CWE-297 Improper Validation of Certificate with Host Mismatch

CVSSv3:
- Base Score: HIGH (7.699999809265137)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

References:
- OSSINDEX - [CVE-2024-34447] CWE-297: Improper Validation of Certificate with Host Mismatch
- OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=CVE%2D2024%2D301XX%20%2D%20When%20endpoint%20identification%20is%20enabled%20in%20the%20BCJSS

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.70:*:*:*:*:*:*:*

CVE-2024-29857 (OSSINDEX) suppress

An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before 1.78, BC Java LTS before 2.73.6, BC-FJA before 1.0.2.5, and BC C# .Net before 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.

CWE-125 Out-of-bounds Read

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:
- OSSINDEX - [CVE-2024-29857] CWE-125: Out-of-bounds Read
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-29857
- OSSIndex - https://github.com/advisories/GHSA-8xfc-gm6g-vgpv
- OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=the%20following%20CVEs%3A-,CVE%2D2024%2D29857,-%2D%20Importing%20an%20EC

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.70:*:*:*:*:*:*:*

CVE-2024-30171 (OSSINDEX) suppress

An issue was discovered in Bouncy Castle Java TLS API and JSSE Provider before 1.78. Timing-based leakage may occur in RSA based handshakes because of exception processing.

CWE-203 Observable Discrepancy

CVSSv3:
- Base Score: MEDIUM (5.900000095367432)
- Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- OSSINDEX - [CVE-2024-30171] CWE-203: Information Exposure Through Discrepancy
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-30171
- OSSIndex - https://github.com/advisories/GHSA-v435-xc8x-wvr9
- OSSIndex - https://github.com/bcgit/bc-java/issues/1528
- OSSIndex - https://www.bouncycastle.org/releasenotes.html#:~:text=during%20parameter%20evaluation.-,CVE%2D2024%2D30171,-%2D%20Possible%20timing%20based

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.70:*:*:*:*:*:*:*

CVE-2023-33202 suppress

Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. (For users of the FIPS Java API: BC-FJA 1.0.2.3 and earlier are affected; BC-FJA 1.0.2.4 is fixed.)

CWE-400 Uncontrolled Resource Consumption

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/E:1.8/RC:R/MAV:A

References:
- OSSINDEX - [CVE-2023-33202] CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-33202
- OSSIndex - https://github.com/bcgit/bc-java/wiki/CVE-2023-33202
- af854a3a-2127-422b-91ae-364da2661108 - EXPLOIT,THIRD_PARTY_ADVISORY
- af854a3a-2127-422b-91ae-364da2661108 - PRODUCT
- af854a3a-2127-422b-91ae-364da2661108 - THIRD_PARTY_ADVISORY
- cve@mitre.org - EXPLOIT,THIRD_PARTY_ADVISORY
- cve@mitre.org - PRODUCT
- cve@mitre.org - THIRD_PARTY_ADVISORY

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:bouncycastle:bouncy_castle_for_java:*:*:*:*:*:*:*:* versions up to (excluding) 1.73
- ...

CVE-2023-33201 (OSSINDEX) suppress

Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability.

CWE-295 Improper Certificate Validation

CVSSv3:
- Base Score: MEDIUM (5.300000190734863)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- OSSINDEX - [CVE-2023-33201] CWE-295: Improper Certificate Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-33201
- OSSIndex - https://github.com/bcgit/bc-java/wiki/CVE-2023-33201

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.bouncycastle:bcprov-jdk15on:1.70:*:*:*:*:*:*:*

spring-core-6.2.9.jar

Description:

Spring Core

License:

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

File Path: C:\Users\eemar\.m2\repository\org\springframework\spring-core\6.2.9\spring-core-6.2.9.jar
MD5: f2761310e5c822d3f9a63e83f890e594
SHA1: 91f5fd4cc7f0bfd27d7b2a5f51b0193ec22c8712
SHA256:9fa0622baf738c9b46f484cdde35c4a97a2a65b1da4426dad0d707d0a8aa3d90
Referenced In Project/Scope: rest-service:compile
Included by: pkg:maven/org.springframework.boot/spring-boot-starter-test@3.5.4

Evidence

Identifiers

- pkg:maven/org.springframework/spring-core@6.2.9 (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:6.2.9:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:springsource:spring_framework:6.2.9:*:*:*:*:*:*:* (*Confidence*:Highest) suppress
- cpe:2.3:a:vmware:spring_framework:6.2.9:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2025-41242 (OSSINDEX) suppress

Spring - Path Traversal

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

CVSSv2:
- Base Score: HIGH (8.199999809265137)
- Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

References:
- OSSINDEX - [CVE-2025-41242] CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-41242
- OSSIndex - https://spring.io/security/cve-2025-41242

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:org.springframework:spring-core:6.2.9:*:*:*:*:*:*:*