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 19:42:34 -0400
- *Dependencies Scanned*: 48 (25 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 1
- *Vulnerabilities Suppressed*: 5 (show)
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence
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	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:*:*:*:*:*:*:*

Suppressed Vulnerabilities

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 Github Advisory Database (via NPM Audit API).
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.