

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

**Sponsor**

## Project: ssl-server

**com.snhu:ssl-server:1.0-SNAPSHOT**

Scan Information (show less):

- *dependency-check version*: 6.5.3
- *Report Generated On*: Wed, 19 Feb 2025 18:04:03 -0500
- *Dependencies Scanned*: 49 (37 unique)
- *Vulnerable Dependencies*: 8
- *Vulnerabilities Found*: 43
- *Vulnerabilities Suppressed*: 164
- *CurrentEngineRelease*: 12.1.0
- *NVD CVE Checked*: 2025-02-19T14:54:21
- *NVD CVE Modified*: 2025-02-19T14:00:03
- *VersionCheckOn*: 2025-02-19T14:54:21

## Summary

Display: Showing Vulnerable Dependencies (click to show all)

| Dependency | Vulnerability IDs | Package | Highest Severity | CVE Count | Confidence | Evidence |
|---|---|---|---|---|---|---|
| json-path-2.4.0.jar | cpe:2.3:a:json-java_project:json-java:2.4.0:*:*:*:*:*:*:* | pkg:maven/com.jayway.jsonpath/json-path@2.4.0 | HIGH | 2 | Low | 29 |
| json-smart-2.3.jar | cpe:2.3:a:ini-parser_project:ini-parser:2.3:*:*:*:*:*:*:*<br>cpe:2.3:a:json-java_project:json-java:2.3:*:*:*:*:*:*:* | pkg:maven/net.minidev/json-smart@2.3 | HIGH | 2 | Low | 34 |
| logback-core-1.2.3.jar | | pkg:maven/ch.qos.logback/logback-core@1.2.3 | MEDIUM | 1 | | 32 |
| spring-boot-starter-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:* | pkg:maven/org.springframework.boot/spring-boot-starter@2.2.4.RELEASE | CRITICAL | 3 | Highest | 26 |
| spring-boot-starter-data-rest-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_data_rest:2.2.4:release:*:*:*:*:*:* | pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE | CRITICAL | 3 | Highest | 26 |
| spring-tx-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:*<br>cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:* | pkg:maven/org.springframework/spring-tx@5.2.3.RELEASE | CRITICAL | 12 | Highest | 26 |
| spring-web-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:* | pkg:maven/org.springframework/spring-web@5.2.3.RELEASE | CRITICAL | 9 | Medium | 26 |
| spring-webmvc-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:* | pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE | CRITICAL | 11 | High | 28 |

## Dependencies

### json-path-2.4.0.jar

**Description:**

Java port of Stefan Goessner JsonPath.

**License:**

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

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

**Evidence**

**Identifiers**

- pkg:maven/com.jayway.jsonpath/json-path@2.4.0 (*Confidence*:High)
- cpe:2.3:a:json-java_project:json-java:2.4.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

**Published Vulnerabilities**

**CVE-2022-45688** suppress

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

CWE-787 Out-of-bounds Write

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

References:
- - https://github.com/dromara/hutool/issues/2748
- - https://github.com/stleary/JSON-java/issues/708

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (excluding) 20230227
- ...

**CVE-2023-5072** suppress

Denial of Service in JSON-Java versions up to and including 20230618. A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.

CWE-770 Allocation of Resources Without Limits or Throttling

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

References:
- - http://www.openwall.com/lists/oss-security/2023/12/13/4
- - https://github.com/stleary/JSON-java/issues/758
- - https://github.com/stleary/JSON-java/issues/771
- - https://security.netapp.com/advisory/ntap-20240621-0007/

Vulnerable Software & Versions:

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

## json-smart-2.3.jar

**Description:**

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

**License:**

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

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

**Evidence**

**Identifiers**

- pkg:maven/net.minidev/json-smart@2.3 (*Confidence*:High)

- cpe:2.3:a:ini-parser_project:ini-parser:2.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress
- cpe:2.3:a:json-java_project:json-java:2.3:*:*:*:*:*:*:* (*Confidence*:Low) suppress

**Published Vulnerabilities**

**CVE-2022-45688** suppress

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

CWE-787 Out-of-bounds Write

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

References:
- - https://github.com/dromara/hutool/issues/2748
- - https://github.com/stleary/JSON-java/issues/708

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:json-java_project:json-java:*:*:*:*:*:*:*:* versions up to (excluding) 20230227
- ...

**CVE-2023-5072** suppress

Denial of Service  in JSON-Java versions up to and including 20230618.  A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.

CWE-770 Allocation of Resources Without Limits or Throttling

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

References:
- - http://www.openwall.com/lists/oss-security/2023/12/13/4
- - https://github.com/stleary/JSON-java/issues/758
- - https://github.com/stleary/JSON-java/issues/771
- - https://security.netapp.com/advisory/ntap-20240621-0007/

Vulnerable Software & Versions:

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

### logback-core-1.2.3.jar

**Description:**

logback-core module

**License:**

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

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

**Evidence**

**Identifiers**

- pkg:maven/ch.qos.logback/logback-core@1.2.3 (*Confidence*:High)

**Published Vulnerabilities**

**CVE-2021-42550** (OSSINDEX) suppress

logback-classic - Deserialization of Untrusted Data [CVE-2021-42550]

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2021-42550 for details

CWE-502 Deserialization of Untrusted Data

CVSSv2:
- Base Score: MEDIUM (6.6)
- Vector: /AV:N/AC:H/Au:/C:H/I:H/A:H

References:
- OSSINDEX - [CVE-2021-42550] CWE-502: Deserialization of Untrusted Data
- OSSIndex - https://jira.qos.ch/browse/LOGBACK-1591

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:ch.qos.logback:logback-core:1.2.3:*:*:*:*:*:*:*

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

**Description:**

Core starter, including auto-configuration support, logging and YAML

**License:**

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

**File Path:** /Users/iancoxon/.m2/repository/org/springframework/boot/spring-boot-starter/2.2.4.RELEASE/spring-boot-starter-2.2.4.RELEASE.jar
**MD5:** d23af33c05bb3f77abf72a08fb227752
**SHA1:** 7a1bb344e00091e7867eb61754fe41f097e13a47
**SHA256:**436ce65593dc1f34efd9dda09cbfa4466c40245b5054e102f3ace3ac56884665
**Referenced In Project/Scope:**ssl-server:compile

**Evidence**

**Related Dependencies**

**Identifiers**

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

**Published Vulnerabilities**

**CVE-2022-27772** suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

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

References:
- - 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

**CVE-2023-20873** suppress

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

NVD-CWE-noinfo

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

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

Vulnerable Software & Versions: (show all)

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

**CVE-2023-20883** suppress

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

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

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

References:
- - https://security.netapp.com/advisory/ntap-20230703-0008/
- - https://spring.io/security/cve-2023-20883

Vulnerable Software & Versions: (show all)

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

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

**Description:**

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

**License:**

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

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

**Evidence**

**Identifiers**

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

**Published Vulnerabilities**

**CVE-2022-27772** suppress

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

CWE-668 Exposure of Resource to Wrong Sphere

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

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

References:
- - 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

**CVE-2023-20873** suppress

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

NVD-CWE-noinfo

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

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

Vulnerable Software & Versions: (show all)

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

**CVE-2023-20883** suppress

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

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

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

References:
- - https://security.netapp.com/advisory/ntap-20230703-0008/
- - https://spring.io/security/cve-2023-20883

Vulnerable Software & Versions: (show all)

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

### spring-tx-5.2.3.RELEASE.jar

**Description:**

Spring Transaction

**License:**

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

**File Path:** /Users/iancoxon/.m2/repository/org/springframework/spring-tx/5.2.3.RELEASE/spring-tx-5.2.3.RELEASE.jar
**MD5:** fab4ecac70d561ceb80c755aed804081
**SHA1:** 99acf44c9844accb84f88672d273ff01527a9592
**SHA256:**ecaad16431f612082f1b8724e45294ed4eee24346acd1a33fb3939018aff60b7
**Referenced In Project/Scope:**ssl-server:compile

**Evidence**

**Related Dependencies**

**Identifiers**

- pkg:maven/org.springframework/spring-tx@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-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:
- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - 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-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:
- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [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
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [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
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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:
- - https://tanzu.vmware.com/security/cve-2021-22060
- - 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:
- - https://security.netapp.com/advisory/ntap-20211125-0005/
- - https://tanzu.vmware.com/security/cve-2021-22096
- - 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
- ...

**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:
- - https://security.netapp.com/advisory/ntap-20210713-0005/
- - https://tanzu.vmware.com/security/cve-2021-22118
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

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

**CVE-2022-22950** suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- - 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-2022-22965** suppress

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

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

CVSSv2:
- Base Score: HIGH (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:
- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220616-0003/
- - https://tanzu.vmware.com/security/cve-2022-22971
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**CVE-2023-20861** suppress

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

NVD-CWE-noinfo

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:
- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 5.2.22
- ...

**CVE-2023-20863** suppress

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

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

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:
- - https://security.netapp.com/advisory/ntap-20240524-0015/
- - https://spring.io/security/cve-2023-20863

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
- ...

### 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:** /Users/iancoxon/.m2/repository/org/springframework/spring-web/5.2.3.RELEASE/spring-web-5.2.3.RELEASE.jar
**MD5:** a89d66690cd14159aa6ac1e875e54411
**SHA1:** dd386a02e40b915ab400a3bf9f586d2dc4c0852c
**SHA256:**25d264969c624cb8103a7f2b36b148ea1be8b87780c4758e7f9a6e2bc8416d76
**Referenced In Project/Scope:**ssl-server:compile

**Evidence**

**Identifiers**

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

**Published Vulnerabilities**

**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:
- - https://tanzu.vmware.com/security/cve-2021-22060
- - 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-2021-22118** 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:
- - https://security.netapp.com/advisory/ntap-20210713-0005/
- - https://tanzu.vmware.com/security/cve-2021-22118
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html
- OSSINDEX - [CVE-2021-22118] CWE-269: Improper Privilege Management
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118
- OSSIndex - https://github.com/spring-projects/spring-framework/issues/26931
- OSSIndex - https://tanzu.vmware.com/security/cve-2021-22118

Vulnerable Software & Versions: (show all)

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

**CVE-2022-22950** suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- - 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-2022-22965** suppress

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

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

CVSSv2:
- Base Score: HIGH (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:
- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:

- - https://security.netapp.com/advisory/ntap-20220616-0003/
- - https://tanzu.vmware.com/security/cve-2022-22971
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**CVE-2023-20861** suppress

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

NVD-CWE-noinfo

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:
- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 5.2.22
- ...

**CVE-2023-20863** suppress

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

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

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:
- - https://security.netapp.com/advisory/ntap-20240524-0015/
- - https://spring.io/security/cve-2023-20863

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
- ...

### 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:** /Users/iancoxon/.m2/repository/org/springframework/spring-webmvc/5.2.3.RELEASE/spring-webmvc-5.2.3.RELEASE.jar
**MD5:** 867cc7369d453637b5042ee4d6931a78
**SHA1:** 745a62502023d2496b565b7fe102bb1ee229d6b7
**SHA256:**b3b0a2477e67b050dd5c08dc96e76db5950cbccba075e782c24f73eda49a0160
**Referenced In Project/Scope:**ssl-server:compile

**Evidence**

**Identifiers**

- pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE (*Confidence*:High)
- cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* (*Confidence*:High) suppress
- cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:* (*Confidence*:High) 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:
- - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-1000027
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-579669626
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-582313417
- - https://github.com/spring-projects/spring-framework/issues/24434#issuecomment-744519525
- - https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000027.json
- - https://security-tracker.debian.org/tracker/CVE-2016-1000027
- - https://security.netapp.com/advisory/ntap-20230420-0009/
- - https://spring.io/blog/2022/05/11/spring-framework-5-3-20-and-5-2-22-available-now
- - 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-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:
- - [ambari-commits] 20201019 [ambari] branch branch-2.7 updated: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421 (dlysnichenko) (#3246)
- - [ambari-dev] 20201019 [GitHub] [ambari] dlysnichenko merged pull request #3246: AMBARI-25571. Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [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
- - [ambari-issues] 20201013 [jira] [Created] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [ambari-issues] 20201021 [jira] [Resolved] (AMBARI-25571) Vulnerable Spring components in Ambari - CVE-2020-5398, CVE-2020-5421
- - [hive-dev] 20201022 [jira] [Created] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Assigned] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20201022 [jira] [Updated] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [hive-issues] 20210107 [jira] [Resolved] (HIVE-24303) Upgrade spring framework to 4.3.29.RELEASE+ due to CVE-2020-5421
- - [ignite-user] 20201117 Query on CVE-2020-5421
- - [ignite-user] 20201119 Re: Query on CVE-2020-5421
- - [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
- - [pulsar-commits] 20201023 [GitHub] [pulsar] Ghatage commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201026 [GitHub] [pulsar] wolfstudy commented on pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [pulsar-commits] 20201028 [GitHub] [pulsar] merlimat merged pull request #8355: [Issue 8354][pulsar-io] Upgrade spring framework version to patch CVE-2020-5421
- - [ranger-dev] 20201007 Re: Review Request 72934: RANGER-3022: Upgrade Spring framework to version 4.3.29.RELEASE
- - https://security.netapp.com/advisory/ntap-20210513-0009/
- - https://tanzu.vmware.com/security/cve-2020-5421
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuApr2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2021.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

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-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:
- - https://security.netapp.com/advisory/ntap-20211125-0005/
- - https://tanzu.vmware.com/security/cve-2021-22096
- - 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
- ...

**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:
- - https://security.netapp.com/advisory/ntap-20210713-0005/
- - https://tanzu.vmware.com/security/cve-2021-22118
- - https://www.oracle.com//security-alerts/cpujul2021.html
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujan2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html
- - https://www.oracle.com/security-alerts/cpuoct2021.html

Vulnerable Software & Versions: (show all)

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

**CVE-2022-22950** suppress

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

CWE-770 Allocation of Resources Without Limits or Throttling

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

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

References:
- - 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-2022-22965** suppress

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

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

CVSSv2:
- Base Score: HIGH (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:
- - 20220401 Vulnerability in Spring Framework Affecting Cisco Products: March 2022
- - http://packetstormsecurity.com/files/166713/Spring4Shell-Code-Execution.html
- - http://packetstormsecurity.com/files/167011/Spring4Shell-Spring-Framework-Class-Property-Remote-Code-Execution.html
- - https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf
- - https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0005
- - https://tanzu.vmware.com/security/cve-2022-22965
- - https://www.kb.cert.org/vuls/id/970766
- - https://www.oracle.com/security-alerts/cpuapr2022.html
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220602-0004/
- - https://tanzu.vmware.com/security/cve-2022-22968
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220616-0006/
- - https://tanzu.vmware.com/security/cve-2022-22970
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**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:
- - https://security.netapp.com/advisory/ntap-20220616-0003/
- - https://tanzu.vmware.com/security/cve-2022-22971
- - https://www.oracle.com/security-alerts/cpujul2022.html

Vulnerable Software & Versions: (show all)

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

**CVE-2023-20861** suppress

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

NVD-CWE-noinfo

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:

- - https://security.netapp.com/advisory/ntap-20230420-0007/
- - https://spring.io/security/cve-2023-20861

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions up to (including) 5.2.22
- ...

**CVE-2023-20863** suppress

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

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

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:
- - https://security.netapp.com/advisory/ntap-20240524-0015/
- - https://spring.io/security/cve-2023-20863

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:vmware:spring_framework:*:*:*:*:*:*:*:* versions from (including) 5.2.0; versions up to (excluding) 5.2.24
- ...

## Suppressed Vulnerabilities

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