

enigma-engine master

M pom.xml

[Overview](#) [History](#) [Settings](#)

Created Sun 22nd Jan 2023
Snapshot taken by snyk.io 15 hours ago

[Retest now](#)

IMPORTED BY

 Djordje Velickovic

PROJECT OWNER

 Add a project owner

ENVIRONMENT

 Add a value

BUSINESS CRITICALITY

 Add a value

LIFECYCLE

 Add a value Search...

Fix these vulnerabilities

63 of 63 issues

Sort by highest priority score ▾

NEW

Did you know...

You can reduce the backlog of existing vulnerabilities at a manageable pace with prioritized fix pull requests - [enable for your GitHub integration](#).

C org.springframework:spring-beans - Remote Code ExecutionSCORE
919VULNERABILITY | [CWE-94](#) | [CVE-2022-22965](#) | [CVSS 9.8](#) **CRITICAL** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-2436751](#)**Insights:** Current public exploits for the Spring4Shell vulnerability require the following conditions:

- Built with Java Runtime Environment (JRE) version 9 or above
- Deployed on either Apache Tomcat, Payara or Glassfish
- Dependent on spring-webmvc or spring-webflux

If your application configuration applies to these conditions, we advise prioritizing remediation of this vulnerability. However, given it is technically possible for additional exploit conditions to exist we do recommend attempting upgrading to a fixed versions for all vulnerable instances.

Introduced through

org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE and others

Fixed in

org.springframework:spring-beans@5.2.20, @5.3.18

Exploit maturity**MATURE**[Show more detail](#) ▾**NEW**[Learn about this type of vulnerability](#)

Ignore

Partially fix this vulnerability

H org.springframework.security:spring-security-web - Authorization Bypass SCORE**731**VULNERABILITY | [CWE-285](#) | [CVE-2022-22978](#) | [CVSS 8.2](#) **HIGH** | [SNYK-JAVA-ORGSPRINGFRAMEWORKSECURITY-2833359](#)**Introduced through**

org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE

Fixed in

org.springframework.security:spring-security-web@5.5.7, @5.6.4

Exploit maturity**PROOF OF CONCEPT**[Show more detail](#) ▾

Ignore

Partially fix this vulnerability

M io.netty:netty-codec-http - HTTP Request SmugglingSCORE
724VULNERABILITY | [CWE-444](#) | [CVE-2021-21295](#) | [CVSS 5.9](#) | MEDIUM | [SNYK-JAVA-IONETTY-1317097](#)


Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-codec-http@4.1.60.Final

Exploit maturity **MATURE**[Show more detail](#) ▾ Ignore Partially fix this vulnerability**M** io.netty:netty-codec-http2 - HTTP Request SmugglingSCORE
724VULNERABILITY | [CWE-444](#) | [CVE-2021-21295](#) | [CVSS 5.9](#) | MEDIUM | [SNYK-JAVA-IONETTY-1083991](#)

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-codec-http2@4.1.60.Final

Exploit maturity **MATURE**[Show more detail](#) ▾ Ignore Partially fix this vulnerability**H** org.postgresql:postgresql - Remote Code Execution (RCE)SCORE
696VULNERABILITY | [CWE-94 + 1 MORE](#) | [CVE-2022-21724](#) | [CVSS 7.5](#) | HIGH | [SNYK-JAVA-ORGPOSTGRESQL-2390459](#)

Introduced through org.postgresql:postgresql@42.2.16

Fixed in org.postgresql:postgresql@42.2.25, @42.3.2

Exploit maturity **PROOF OF CONCEPT**[Show more detail](#) ▾

NEW


 [Learn about this type of vulnerability](#) Ignore Partially fix this vulnerability

org.keycloak:keycloak-core - Improper Authorization

SCORE
691VULNERABILITY | [CWE-285](#) | [CVE-2022-1466](#) | [CVSS 7.4](#) **HIGH** | [SNYK-JAVA-ORGKEYCLOAK-2805802](#)

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2

Fixed in org.keycloak:keycloak-core@17.0.1


Exploit maturity **PROOF OF CONCEPT**[Show more detail](#) ▼ Ignore Fix this vulnerability

org.bouncycastle:bcprov-jdk15on - Comparison Using Wrong Factors

SCORE
686VULNERABILITY | [CWE-1025](#) | [CVE-2020-28052](#) | [CVSS 7.3](#) **HIGH** | [SNYK-JAVA-ORGBOUNCYCASTLE-1052448](#)

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2

Fixed in org.bouncycastle:bcprov-jdk15on@1.67

Exploit maturity **PROOF OF CONCEPT**[Show more detail](#) ▼ Ignore Fix this vulnerability

org.liquibase:liquibase-core - XML External Entity (XXE) Injection

SCORE
686VULNERABILITY | [CWE-611](#) | [CVE-2022-0839](#) | [CVSS 7.3](#) **HIGH** | [SNYK-JAVA-ORGLIQUIBASE-2419059](#)

Introduced through org.liquibase:liquibase-core@3.8.9

Fixed in org.liquibase:liquibase-core@4.8.0

Exploit maturity **PROOF OF CONCEPT**[Show more detail](#) ▼ Ignore Partially fix this vulnerability



org.postgresql:postgresql - SQL Injection

VULNERABILITY | [CWE-89](#) | [CVE-2022-31197](#) | [CVSS 7.1](#)  | [SNYK-JAVA-ORGPOSTGRESQL-2970521](#)

SCORE
676

Introduced through `org.postgresql:postgresql@42.2.16`
Fixed in `org.postgresql:postgresql@42.2.26, @42.3.7, @42.4.1`
Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾

  [Learn about this type of vulnerability](#)


 Ignore

 Partially fix this vulnerability

org.hibernate:hibernate-core - SQL Injection



VULNERABILITY | [CWE-89](#) | [CVE-2020-25638](#) | [CVSS 8.2](#)  | [SNYK-JAVA-ORGHIBERNATE-1041788](#)


SCORE
635

 **Insights:** This vulnerability is only applicable on systems using JPA Criteria API

Introduced through `org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE`
Fixed in `org.hibernate:hibernate-core@5.4.24.Final`
Exploit maturity **NO KNOWN EXPLOIT**

Show more detail ▾

  [Learn about this type of vulnerability](#)

 Ignore

 Partially fix this vulnerability

org.keycloak:keycloak-core - Cross-site Scripting (XSS)

SCORE
629VULNERABILITY | [CWE-79](#) | [CVE-2021-20195](#) | [CVSS 8.3](#) **HIGH** | [SNYK-JAVA-ORGKEYCLOAK-1075058](#)



Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2

Fixed in org.keycloak:keycloak-core@13.0.0

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

NEW

 [Learn about this type of vulnerability](#) Ignore Fix this vulnerability

org.keycloak:keycloak-core - Cross-site Scripting (XSS)

SCORE
629VULNERABILITY | [CWE-79](#) | [CVE-2021-20222](#) | [CVSS 8.3](#) **HIGH** | [SNYK-JAVA-ORGKEYCLOAK-1075057](#)


Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2

Fixed in org.keycloak:keycloak-core@13.0.0

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

NEW

 [Learn about this type of vulnerability](#) Ignore Fix this vulnerability

org.postgresql:postgresql - Arbitrary Code Injection

SCORE
619VULNERABILITY | [CWE-94](#) | [CVE-2022-26520](#) | [CVSS 8.1](#) **HIGH** | [SNYK-JAVA-ORGPOSTGRESQL-2401816](#)

Introduced through org.postgresql:postgresql@42.2.16

Fixed in org.postgresql:postgresql@42.3.3

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

NEW

 [Learn about this type of vulnerability](#) Ignore Partially fix this vulnerability

M **com.fasterxml.jackson.core:jackson-databind** - Denial of Service (DoS)

VULNERABILITY | [CWE-400](#) | [CVE-2022-42003](#) | [CVSS 5.9](#) **MEDIUM** | [SNYK-JAVA-COMFASTERXMLJACKSONCORE-3038426](#)

SCORE
616

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2 and org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in com.fasterxml.jackson.core:jackson-databind@2.12.7.1, @2.13.4.2

Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾

 Ignore

 Partially fix this vulnerability

M **com.fasterxml.jackson.core:jackson-databind** - Denial of Service (DoS)

VULNERABILITY | [CWE-400](#) | [CVE-2022-42004](#) | [CVSS 5.9](#) **MEDIUM** | [SNYK-JAVA-COMFASTERXMLJACKSONCORE-3038424](#)

SCORE
616

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2 and org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in com.fasterxml.jackson.core:jackson-databind@2.13.4

Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾

 Ignore

 Partially fix this vulnerability

M **org.keycloak:keycloak-core** - Cross-site Scripting (XSS)

VULNERABILITY | [CWE-79](#) | [CVE-2021-20323](#) | [CVSS 5.4](#) **MEDIUM** | [SNYK-JAVA-ORGKEYCLOAK-2434281](#)


SCORE
591

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2


Fixed in org.keycloak:keycloak-core@17.0.0

Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾

NEW  [Learn about this type of vulnerability](#)

 Ignore

 Fix this vulnerability

**com.fasterxml.jackson.core:jackson-databind** - Denial of Service (DoS)

SCORE

589VULNERABILITY | [CWE-400](#) | [CVE-2020-36518](#) | [CVSS 7.5](#) **HIGH** | [SNYK-JAVA-COMFASTERXMLJACKSONCORE-2421244](#)**Insights:** This vulnerability is only applicable when using nested objects.**Introduced through**

org.keycloak:keycloak-spring-boot-starter@11.0.2 and org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in

com.fasterxml.jackson.core:jackson-databind@2.12.6.1, @2.13.2.1

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾



Ignore



Partially fix this vulnerability

**io.netty:netty-codec** - Denial of Service (DoS)

SCORE

589VULNERABILITY | [CWE-400](#) | [CVE-2021-37136](#) | [CVSS 7.5](#) **HIGH** | [SNYK-JAVA-IONETTY-1584064](#)**Introduced through**

org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in

io.netty:netty-codec@4.1.68.Final

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾



Ignore



Partially fix this vulnerability

**io.netty:netty-codec** - Denial of Service (DoS)

SCORE

589VULNERABILITY | [CWE-400](#) | [CVE-2021-37137](#) | [CVSS 7.5](#) **HIGH** | [SNYK-JAVA-IONETTY-1584063](#)**Introduced through**

org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in

io.netty:netty-codec@4.1.68.Final

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾




Ignore



Partially fix this vulnerability


org.apache.tomcat.embed:tomcat-embed-core - Denial of Service (DoS) SCORE 589

VULNERABILITY | [CWE-400](#) | [CVE-2021-41079](#) | [CVSS 7.5](#) HIGH | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1728264](#)

 **Insights:** This vulnerability is only applicable on Tomcat configured with NIO/NIO2 Connectors + OpenSSL and systems based on the PowerPC CPU architecture

Introduced through `org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE`
Fixed in `org.apache.tomcat.embed:tomcat-embed-core@10.0.4, @8.5.64, @9.0.44`
Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

 Ignore


 Partially fix this vulnerability

org.yaml:snakeyaml - Denial of Service (DoS) SCORE 589

VULNERABILITY | [CWE-400](#) | [CVE-2022-25857](#) + 1 MORE | [CVSS 7.5](#) HIGH | [SNYK-JAVA-ORGYAML-2806360](#)

Introduced through `org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE`
Fixed in `org.yaml:snakeyaml@1.31`
Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

 Ignore

 Partially fix this vulnerability

org.apache.tomcat.embed:tomcat-embed-core - Information Exposure SCORE 586

VULNERABILITY | [CWE-200](#) | [CVE-2020-17527](#) | [CVSS 5.3](#) MEDIUM | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1048292](#)

Introduced through `org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE`
Fixed in `org.apache.tomcat.embed:tomcat-embed-core@8.5.60, @9.0.40, @10.0.0-M10`
Exploit maturity PROOF OF CONCEPT

Show more detail ▾

 Ignore

 Partially fix this vulnerability


org.glassfish:jakarta.el - Improper Input Validation

SCORE
579VULNERABILITY | [CWE-20](#) | [CVE-2021-28170](#) | [CVSS 7.3](#) **HIGH** | [SNYK-JAVA-ORGGLASSFISH-1297098](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.glassfish:jakarta.el@3.0.4

Exploit maturity NO KNOWN EXPLOIT

[Show more detail](#) ▾ Ignore Partially fix this vulnerability

org.apache.tomcat.embed:tomcat-embed-core - Privilege Escalation

SCORE
564VULNERABILITY | [CWE-264](#) | [CVE-2022-23181](#) | [CVSS 7](#) **HIGH** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-2414084](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.apache.tomcat.embed:tomcat-embed-core@8.5.75, @9.0.58, @10.0.16, @10.1.0-M10

Exploit maturity NO KNOWN EXPLOIT

[Show more detail](#) ▾ Ignore Partially fix this vulnerability

org.apache.tomcat.embed:tomcat-embed-core - Remote Code Execution (RCE)

SCORE
564VULNERABILITY | [CWE-94](#) | [CVE-2021-25329](#) | [CVSS 7](#) **HIGH** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1080637](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.apache.tomcat.embed:tomcat-embed-core@10.0.2, @9.0.43, @8.5.63, @7.0.108

Exploit maturity NO KNOWN EXPLOIT

[Show more detail](#) ▾

NEW

 [Learn about this type of vulnerability](#) Ignore Partially fix this vulnerability



M org.bouncycastle:bcprov-jdk15on - Cryptographic IssuesSCORE
561VULNERABILITY | [CWE-310](#) | [CVSS 4.8](#) | **MEDIUM** | [SNYK-JAVA-ORGBOUNCYCASTLE-2841508](#)

Introduced through org.keycloak:keycloak-spring-boot-starter@11.0.2

Fixed in org.bouncycastle:bcprov-jdk15on@1.69

Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾


NEW  [Learn about this type of vulnerability](#) Ignore Fix this vulnerability**M** io.netty:netty-codec-http - Denial of Service (DoS)SCORE
539VULNERABILITY | [CWE-400](#) | [CVSS 6.5](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-1020439](#)

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-codec-http@4.1.53.Final

Exploit maturity **NO KNOWN EXPLOIT**

Show more detail ▾

 Ignore Partially fix this vulnerability**M** io.netty:netty-codec-http - HTTP Request SmugglingSCORE
539VULNERABILITY | [CWE-444](#) | [CVE-2021-43797](#) | [CVSS 6.5](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-2314893](#)

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-codec-http@4.1.71.Final

Exploit maturity **NO KNOWN EXPLOIT**

Show more detail ▾

 Ignore Partially fix this vulnerability



M org.yaml:snakeyaml - Stack-based Buffer OverflowSCORE
536VULNERABILITY | [CWE-121](#) | [CVE-2022-38751](#) | [CVSS 4.3](#) | MEDIUM | [SNYK-JAVA-ORGYAML-3016891](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.yaml:snakeyaml@1.31

Exploit maturity **PROOF OF CONCEPT**

Show more detail ▾


 Ignore Partially fix this vulnerability**M** io.netty:netty-codec-http - Information DisclosureSCORE
524VULNERABILITY | [CWE-378](#) | [CVE-2021-21290](#) | [CVSS 6.2](#) | MEDIUM | [SNYK-JAVA-IONETTY-1070799](#) **Insights:** This vulnerability is only applicable on Unix-based operating systems

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-codec-http@4.1.59.Final

Exploit maturity **NO KNOWN EXPLOIT**

Show more detail ▾

 Ignore Partially fix this vulnerability**M** io.netty:netty-common - Information DisclosureSCORE
524VULNERABILITY | [CWE-378](#) | [CVE-2021-21290](#) | [CVSS 6.2](#) | MEDIUM | [SNYK-JAVA-IONETTY-1082234](#) **Insights:** This vulnerability is only applicable on Unix-based operating systems


Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-common@4.1.59.Final

Exploit maturity **NO KNOWN EXPLOIT**

Show more detail ▾

 Ignore Partially fix this vulnerability



M **io.netty:netty-handler** - Information DisclosureSCORE
524VULNERABILITY | [CWE-378](#) | [CVE-2021-21290](#) | [CVSS 6.2](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-1082235](#) **Insights:** This vulnerability is only applicable on Unix-based operating systems

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-handler@4.1.59.Final

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾



 Ignore Partially fix this vulnerability**M** **io.netty:netty-transport** - Information DisclosureSCORE
524VULNERABILITY | [CWE-378](#) | [CVE-2021-21290](#) | [CVSS 6.2](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-1082236](#) **Insights:** This vulnerability is only applicable on Unix-based operating systems

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-transport@4.1.59.Final

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾


 Ignore Partially fix this vulnerability**M** **io.netty:netty-transport-native-epoll** - Information DisclosureSCORE
524VULNERABILITY | [CWE-378](#) | [CVE-2021-21290](#) | [CVSS 6.2](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-1082238](#) **Insights:** This vulnerability is only applicable on Unix-based operating systems

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in io.netty:netty-transport-native-epoll@4.1.59.Final

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

 Ignore Partially fix this vulnerability

M **com.fasterxml.jackson.core:jackson-databind** - Denial of Service (DoS)SCORE
509VULNERABILITY | [CWE-400](#) | [CVSS 5.9](#) **MEDIUM** | [SNYK-JAVA-COMFASTERXMLJACKSONCORE-2326698](#)**Insights:** This vulnerability is only applicable when JDK serialization ("ObjectInputStream" or "ObjectOutputStream", as opposed to Jackson serialization) is in use.

Introduced through

org.keycloak:keycloak-spring-boot-starter@11.0.2 and org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

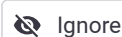
Fixed in

com.fasterxml.jackson.core:jackson-databind@2.13.1, @2.12.6

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾



Ignore



Partially fix this vulnerability

M **io.netty:netty-codec-http2** - HTTP Request SmugglingSCORE
509VULNERABILITY | [CWE-444](#) | [CVE-2021-21409](#) | [CVSS 5.9](#) **MEDIUM** | [SNYK-JAVA-IONETTY-1089809](#)

Introduced through

org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Fixed in

io.netty:netty-codec-http2@4.1.61.Final

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾



Ignore



Partially fix this vulnerability

M **org.apache.tomcat.embed:tomcat-embed-core** - HTTP Request SmugglingSCORE
509VULNERABILITY | [CWE-444](#) | [CVE-2021-25122](#) | [CVSS 5.9](#) **MEDIUM** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1080638](#)

Introduced through

org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

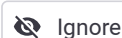
Fixed in

org.apache.tomcat.embed:tomcat-embed-core@10.0.2, @9.0.43, @8.5.63

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾



Ignore



Partially fix this vulnerability


org.springframework:spring-context - Improper Handling of Case Sensitivity

VULNERABILITY | [CWE-178](#) | [CVE-2022-22968](#) | [CVSS 3.7](#)  | [SNYK-JAVA-ORSPRINGFRAMEWORK-2689634](#)


SCORE **506**


Introduced through org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE and others

Fixed in org.springframework:spring-context@5.2.21, @5.3.19

Exploit maturity 

Show more detail ▾

 Ignore

 Partially fix this vulnerability


org.yaml:snakeyaml - Stack-based Buffer Overflow

VULNERABILITY | [CWE-121](#) | [CVE-2022-38752](#) | [CVSS 3.7](#)  | [SNYK-JAVA-ORGYAML-3016888](#)


SCORE **506**

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.yaml:snakeyaml@1.32

Exploit maturity 

Show more detail ▾


 Ignore

 Partially fix this vulnerability

io.netty:netty-common - Information Exposure

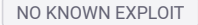
VULNERABILITY | [CWE-200 + 1 MORE](#) | [CVE-2022-24823](#) | [CVSS 5.5](#)  | [SNYK-JAVA-IONETTY-2812456](#)

SCORE **489**


 **Insights:** This vulnerability is only applicable on systems using Java 6 and below

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE



Fixed in io.netty:netty-common@4.1.77.Final

Exploit maturity 

Show more detail ▾

 Ignore


 Partially fix this vulnerability

M **org.keycloak:keycloak-core** - Improper Access ControlSCORE
484VULNERABILITY | [CWE-284](#) | [CVE-2020-1725](#) | [CVSS 5.4](#) | **MEDIUM** | [SNYK-JAVA-ORGKEYCLOAK-1061995](#)Introduced through `org.keycloak:keycloak-spring-boot-starter@11.0.2`Fixed in `org.keycloak:keycloak-core@13.0.0`Exploit maturity **NO KNOWN EXPLOIT**[Show more detail](#) ▾ Ignore Fix this vulnerability**M** **org.apache.httpcomponents:httpclient** - Improper Input ValidationSCORE
479VULNERABILITY | [CWE-20](#) | [CVE-2020-13956](#) | [CVSS 5.3](#) | **MEDIUM** | [SNYK-JAVA-ORGAPACHEHTTPCOMPONENTS-1048058](#)Introduced through `org.keycloak:keycloak-spring-boot-starter@11.0.2`Fixed in `org.apache.httpcomponents:httpclient@4.5.13`Exploit maturity **NO KNOWN EXPLOIT**[Show more detail](#) ▾ Ignore Fix this vulnerability**M** **org.apache.tomcat.embed:tomcat-embed-core** - HTTP Request SmugglingSCORE
479VULNERABILITY | [CWE-444](#) | [CVE-2021-33037](#) | [CVSS 5.3](#) | **MEDIUM** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1728266](#)Introduced through `org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE`Fixed in `org.apache.tomcat.embed:tomcat-embed-core@10.0.7, @9.0.48, @8.5.68`Exploit maturity **NO KNOWN EXPLOIT**[Show more detail](#) ▾ Ignore Partially fix this vulnerability

M **org.apache.tomcat.embed:tomcat-embed-core** - Information Disclosure

VULNERABILITY | [CWE-200](#) | [CVE-2021-24122](#) | [CVSS 5.3](#) **MEDIUM** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1061939](#)

SCORE
479

 **Insights:** This vulnerability is only applicable on Windows operating system

Introduced through `org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE`

Fixed in `org.apache.tomcat.embed:tomcat-embed-core@10.0.0-M10, @9.0.40, @8.5.60, @7.0.107`

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

[Ignore](#)[Partially fix this vulnerability](#)

M **org.bouncycastle:bcprov-jdk15on** - Timing Attack

VULNERABILITY | [CWE-208](#) | [CVE-2020-15522](#) | [CVSS 5.3](#) **MEDIUM** | [SNYK-JAVA-ORGBOUNCYCASTLE-1296075](#)

SCORE
479

Introduced through `org.keycloak:keycloak-spring-boot-starter@11.0.2`

Fixed in `org.bouncycastle:bcprov-jdk15on@1.66`

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

[Ignore](#)[Fix this vulnerability](#)

M **org.springframework:spring-beans** - Denial of Service (DoS)

VULNERABILITY | [CWE-400](#) | [CVE-2022-22970](#) | [CVSS 5.3](#) **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-2823313](#)

SCORE
479

Introduced through `org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE` and others

Fixed in `org.springframework:spring-beans@5.2.22.RELEASE, @5.3.20`

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

[Ignore](#)[Partially fix this vulnerability](#)

M org.springframework:spring-expression - Denial of Service (DoS)SCORE
479VULNERABILITY | [CWE-400](#) | [CVE-2022-22950](#) | [CVSS 5.3](#) **MEDIUM** | [SNYK-JAVA-ORGSRINGFRAMEWORK-2434828](#)**Insights:** This vulnerability is only applicable on systems using Spring Expression Language (SpEL)**Introduced through** org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE and org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE**Fixed in** org.springframework:spring-expression@5.2.20.RELEASE, @5.3.17**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

Ignore

Partially fix this vulnerability

M ch.qos.logback:logback-core - Insufficient Hostname VerificationSCORE
454VULNERABILITY | [CWE-20](#) | [CVSS 4.8](#) **MEDIUM** | [SNYK-JAVA-CHQOSLOGBACK-1726923](#)**Introduced through** org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE**Fixed in** ch.qos.logback:logback-core@1.2.7**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

Ignore

Partially fix this vulnerability

M org.apache.tomcat.embed:tomcat-embed-core - Improper Input Validation SCORE
454VULNERABILITY | [CWE-20](#) | [CVE-2021-30640](#) | [CVSS 4.8](#) **MEDIUM** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-1728265](#)**Introduced through** org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE**Fixed in** org.apache.tomcat.embed:tomcat-embed-core@10.0.6, @9.0.46, @8.5.66, @7.0.109**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

Ignore


Partially fix this vulnerability

M org.postgresql:postgresql - Information ExposureSCORE
449VULNERABILITY | [CWE-200](#) | [CVE-2022-41946](#) | [CVSS 4.7](#) | **MEDIUM** | [SNYK-JAVA-ORGPSTGRESQL-3146847](#)

Introduced through org.postgresql:postgresql@42.2.16

Fixed in org.postgresql:postgresql@42.2.27, @42.3.8, @42.4.3, @42.5.1


Exploit maturity **NO KNOWN EXPLOIT**

[Show more detail](#) ▾ Ignore Partially fix this vulnerability**M** org.springframework.security:spring-security-core - Privilege EscalationSCORE
439VULNERABILITY | [CWE-264](#) | [CVE-2021-22112](#) | [CVSS 4.5](#) | **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORKSECURITY-1078232](#)

Introduced through org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE

Fixed in org.springframework.security:spring-security-core@5.4.4, @5.3.8.RELEASE, @5.2.9.RELEASE

Exploit maturity **NO KNOWN EXPLOIT**

[Show more detail](#) ▾ Ignore Partially fix this vulnerability**M** org.springframework:spring-web - Privilege EscalationSCORE
434VULNERABILITY | [CWE-264](#) | [CVE-2021-22118](#) | [CVSS 4.4](#) | **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-1296829](#)

Introduced through org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE and others


Fixed in org.springframework:spring-web@5.3.7, @5.2.15.RELEASE

Exploit maturity **NO KNOWN EXPLOIT**


[Show more detail](#) ▾ Ignore Partially fix this vulnerability

M org.springframework:spring-core - Improper Input ValidationSCORE
429VULNERABILITY | [CWE-20](#) | [CVE-2021-22060](#) | [CVSS 4.3](#) **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-2330878](#)**Introduced through** org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE and others**Fixed in** org.springframework:spring-core@5.2.19.RELEASE, @5.3.14**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

 Ignore Partially fix this vulnerability**M** org.springframework:spring-core - Improper Output Neutralization for LogsSCORE
429VULNERABILITY | [CWE-20](#) | [CVE-2021-22096](#) | [CVSS 4.3](#) **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-2329097](#)**Introduced through** org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE, org.springframework.boot:spring-boot-starter-data-jpa@2.3.4.RELEASE and others**Fixed in** org.springframework:spring-core@5.3.12, @5.2.18**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

 Ignore Partially fix this vulnerability**M** org.springframework:spring-webflux - Improper Output Neutralization for LogsSCORE
429VULNERABILITY | [CWE-20](#) | [CVE-2021-22096](#) | [CVSS 4.3](#) **MEDIUM** | [SNYK-JAVA-ORGSPRINGFRAMEWORK-2329098](#)**Introduced through** org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE**Fixed in** org.springframework:spring-webflux@5.3.12, @5.2.18**Exploit maturity** NO KNOWN EXPLOIT

Show more detail ▾

 Ignore Partially fix this vulnerability

org.apache.tomcat.embed:tomcat-embed-core - HTTP Request Smuggling


VULNERABILITY | [CWE-444](#) | [CVE-2022-42252](#) | [CVSS 3.7](#) **LOW** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-3097829](#)

SCORE
399

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.apache.tomcat.embed:tomcat-embed-core@8.5.53, @9.0.68, @10.0.27, @10.1.1

Exploit maturity **NO KNOWN EXPLOIT**

[Show more detail](#) ▼ Ignore Partially fix this vulnerability

org.apache.tomcat.embed:tomcat-embed-core - Information Exposure


VULNERABILITY | [CWE-200](#) | [CVE-2021-43980](#) | [CVSS 3.7](#) **LOW** | [SNYK-JAVA-ORGAPACHETOMCATEMBED-3035793](#)

SCORE
399

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.apache.tomcat.embed:tomcat-embed-core@8.5.78, @9.0.62, @10.0.20, @10.1.0-M14

Exploit maturity **NO KNOWN EXPLOIT**

[Show more detail](#) ▼ Ignore Partially fix this vulnerability

org.yaml:sakeyaml - Stack-based Buffer Overflow


VULNERABILITY | [CWE-121](#) | [CVE-2022-41854](#) | [CVSS 3.7](#) **LOW** | [SNYK-JAVA-ORGYAML-3113851](#)

SCORE
399

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.yaml:sakeyaml@1.32

Exploit maturity **NO KNOWN EXPLOIT**

[Show more detail](#) ▼ Ignore Partially fix this vulnerability


L org.yaml:snakeyaml - Stack-based Buffer OverflowSCORE
399VULNERABILITY | [CWE-121](#) | [CVE-2022-38750](#) | [CVSS 3.7](#) **LOW** | [SNYK-JAVA-ORGYAML-3016889](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Fixed in org.yaml:snakeyaml@1.31

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾


 Ignore Partially fix this vulnerability**L** org.springframework.security:spring-security-web - Timing AttackSCORE
380VULNERABILITY | [CWE-208](#) | [CVSS 3.1](#) **LOW** | [SNYK-JAVA-ORGSPRINGFRAMEWORKSECURITY-1290497](#)

Introduced through org.springframework.boot:spring-boot-starter-security@2.3.4.RELEASE

Fixed in org.springframework.security:spring-security-web@5.2.9.RELEASE, @5.3.7, @5.4.3

Exploit maturity NO KNOWN EXPLOIT


Show more detail ▾

 Ignore Partially fix this vulnerability**M** org.yaml:snakeyaml - Arbitrary Code ExecutionSCORE
330VULNERABILITY | [CWE-20](#) | [CVE-2022-1471](#) | [CVSS 6.6](#) **MEDIUM** | [SNYK-JAVA-ORGYAML-3152153](#)

Introduced through org.springframework.boot:spring-boot-starter-web@2.3.4.RELEASE

Exploit maturity NO KNOWN EXPLOIT

Show more detail ▾

 Ignore

M **io.netty:netty-handler** - Improper Certificate ValidationSCORE
291VULNERABILITY | [CWE-295](#) | [CVSS 5.6](#) | **MEDIUM** | [SNYK-JAVA-IONETTY-1042268](#)**Insights:** This vulnerability is only applicable when certificate hostname validation is disabled.

Introduced through

org.springframework.boot:spring-boot-starter-webflux@2.3.4.RELEASE

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾

Ignore

L **org.keycloak:keycloak-core** - Improper Input ValidationSCORE
185VULNERABILITY | [CWE-20](#) | [CVE-2021-3754](#) | [CVSS 3.7](#) | **LOW** | [SNYK-JAVA-ORGKEYCLOAK-3026902](#)

Introduced through

org.keycloak:keycloak-spring-boot-starter@11.0.2

Exploit maturity

NO KNOWN EXPLOIT

Show more detail ▾

Ignore