Spring Framework - CVE vulnerabilities

⚠ This page will be updated over the coming days as and when new information is available.

Introduction

Two Remote Code Execution vulnerabilities (RCE) have been found recently in **Spring Framework** (the java based application framework):

- **CVE-2022-22963 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-22963** and **https://tanzu.vmware.com/security/cve-2022-22963**
- **CVE-2022-22965 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-22965** and **https://tanzu.vmware.com/security/cve-2022-22965** (known as Spring4Shell)

See also:

- **https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement**
- **https://www.lunasec.io/docs/blog/spring-rce-vulnerabilities/**

CVE-2022-22963

In summary, any java application that uses the following is potentially vulnerable to this CVE:

- Spring Cloud Function versions:
  - 3.1.6
  - 3.2.2
  - Older, unsupported versions are also affected

Spring have fixed this vulnerability in the following releases:

- **Spring Cloud Function 3.1.7** and **3.2.3**

CVE-2022-22965

In summary, any java application that uses the following combination of items is potentially vulnerable to this CVE:

- Java JDK 9 or higher
- Apache Tomcat as the Servlet container
- Packaged as a traditional WAR (in contrast to a Spring Boot executable jar)
- `spring-webmvc` or `spring-webflux` dependency
- Spring Framework versions
  - 5.3.0 to 5.3.17
  - 5.2.0 to 5.2.19
  - Older, unsupported versions are also affected

Spring have fixed this vulnerability in the following releases:

- **Spring Framework 5.3.18** and **5.2.20**
- **Spring Boot 2.6.6** and **2.5.12** that depend on **Spring Framework 5.3.18**

What information does this page provide?

CAST makes use of **Spring Framework / Spring Boot / Spring Cloud Function** in various products, therefore this page explains:

- which products are affected by these vulnerabilities
- how CAST plans to mitigate the threat

Which CAST products are affected?

Product	CVE-2022-22963	CVE-2022-22965
CAST Dashboards (standalone and embedded via the integrated RestAPI)	Not affected (Spring Cloud is used in 2.x, however, the Spring Cloud Function itself is not used).	All releases (when deployed on Apache Tomcat via a WAR file AND with Java 9 or above).
AIP Core	Not affected.	Not affected.
CAST Imaging	Not affected.	Not affected.
AIP Console/AIP Node	Not affected (Spring Cloud is used in 2.x, however, the Spring Cloud Function itself is not used).	Not affected (impacted Spring Framework JARs are used in all releases, however, they are not deployed via a traditional WAR).
CAST official extensions	Not affected.	Not affected.

How does CAST plan to mitigate the threat?

CAST will release updates to affected products in the coming days - these updates will contain **Spring Framework 5.3.18** / **5.2.20** and/or **Spring Boot 2.6.6** / **2.5.12** which fix the vulnerabilities. Only the most recent releases of each affected product will be patched, therefore this necessarily means upgrading to the newest release to receive the patch (CAST highly recommends this in all situations where possible).

Affected Product	Release containing fixes for CVE-2022-22965	Detail of fixes provided
CAST Dashboards (standalone)	**2.6.1-funcrel** Released **08 April 2022**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard&version=2.6.1-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.health&version=2.6.1-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.engineering&version=2.6.1-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.security&version=2.6.1-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.restapi&version=2.6.1-funcrel**	• **Spring Framework** upgraded to **5.3.18** • **Spring Boot** upgraded to **2.5.12**
	1.28.7-funcrel Released **08 April 2022**. • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.health&version=1.28.7-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard&version=1.28.7-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.engineering&version=1.28.7-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.restapi&version=1.28.7-funcrel** • **https://extend.castsoftware.com/#/extension?id=com.castsoftware.aip.dashboard.security&version=1.28.7-funcrel**	• **Spring Framework** upgraded to **5.3.18** • **Spring Boot** is not used.

What you can do to prevent the vulnerability from being exploited?

If you are waiting for a patch from CAST for an impacted product, or you cannot upgrade to the CAST product release containing **Spring Framework 5.3.18** / **5.2.20** **Spring Boot 2.6.6** / **2.5.12**, you can perform the action listed below to mitigate the vulnerability.

Upgrade Apache Tomcat to mitigate CVE-2022-22965

Apache has released updates to **Apache Tomcat** which mitigate the threat posed by **CVE-2022-22965** as discussed in **https://spring.io/blog/2022/04/01/spring-framework-rce-mitigation-alternative**. The CVE is not present in Apache Tomcat, however, the new releases include a change to disable the `We bappClassLoaderBase.getResources()` method which prevents **CVE-2022-22965** from being exploited.

Therefore, CAST highly recommends upgrading your deployed Apache Tomcat to the following releases (**supported** by CAST for deployment of CAST Dashboards/RestAPI) wherever possible:

- **9.0.62** (see release notes here: **https://tomcat.apache.org/tomcat-9.0-doc/changelog.html**)
- **8.5.78** (see release notes here: **https://tomcat.apache.org/tomcat-8.5-doc/changelog.html**)