CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+

CRITICAL | MARCH 31, 2022 | CVE-2022-22965

Description

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.

These are the prerequisites for the exploit:

- JDK 9 or higher
- Apache Tomcat as the Servlet container
- Packaged as WAR
- spring-webmvc or spring-webflux dependency

Affected Spring Products and Versions

- Spring Framework
  - 5.3.0 to 5.3.17
  - 5.2.0 to 5.2.19
  - Older, unsupported versions are also affected

Mitigation

Users of affected versions should apply the following mitigation: 5.3.x users should upgrade to 5.3.18+, 5.2.x users should upgrade to 5.2.20+. No other steps are

necessary. There are other mitigation steps for applications that cannot upgrade to the above versions. Those are described in the early announcement blog post, listed under the Resources section. Releases that have fixed this issue include:

- Spring Framework
  - 5.3.18+
  - 5.2.20+

Credit

This vulnerability was responsibly reported to VMware by codeplutos, meizjm3i of AntGroup FG Security Lab. A secondary report was also received from Praetorian.

References

- https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
- https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

History

- 2022-03-31: Initial vulnerability report published.

Reporting a vulnerability

To report a security vulnerability for a project within the Spring portfolio, see the Security Policy