

Threat Bulletin

Spring4Shell

Summary

Update – Thursday, March 31 12:15pm:

Patches are now available.

- 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.

Update - Thursday, March 31: VMware has [posted some CVE information](#), CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+.

Spring4Shell was disclosed on Tuesday, March 29th. This vulnerability should not be confused with CVE-2022-22963 or CVE-2022-27772, two other Spring framework vulnerabilities. Spring4Shell is caused by unsafe [deserialization](#) of passed arguments.

Spring.io posted an announcement on their blog, [Spring Framework RCE, Early Announcement](#).

Are you impacted? 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

A remediation workaround has been [posted by SpringCloud.io](#).

At 3:33am EDT, LunaSec updated their blog post with a writeup covering exploitation details.

At 6:38pm EDT, [LunaSec posted on Twitter](#) that they updated their [blog post](#) with more details about Spring4Shell.

We don't have information on how widespread or exploitable this vulnerability is but [Praetorian has confirmed that it is exploitable](#).

Official notice from the Spring project will likely be posted on the [VMware Tanzu security advisories](#) webpage.



Vendor: Java Spring Framework

CVE-ID: CVE-2022-22965

Published: 03/30/2022

CVSS V3 Overall score: TBD

Criticality: High

Patch Availability: Yes

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: TBD

Attack Complexity: TBD

Privileges Required: TBD

User Interaction: TBD

Impact Metrics

Scope: TBD

Confidentiality: TBD

Integrity: TBD

Availability: TBD

Confidence Metrics

Exploitability: TBD

Remediation Level: TBD

Report Confidence: TBD



Wednesday, March 30: An **unconfirmed** zero-day vulnerability referred to as Spring4Shell was posted on multiple websites and has been getting a lot of attention. CVE details are not currently available. We expect more details to be made available over the next 10-24 hours.

The vulnerability exists in the Spring framework with JDK version greater or equal to 9.0. Multiple proof-of-concepts have been posted online but remain unconfirmed.

Affected Products

Spring Framework

- 5.3.0 to 5.3.17
- 5.2.0 to 5.2.19

Safeguards/Recommendations

Update – Thursday, March 31:

Patches are available.

- 5.3.x users should upgrade to 5.3.18+
- 5.2.x users should upgrade to 5.2.20+

Developers should know [how to prevent deserialization attacks](#).

Wednesday 29: We recommend organizations implement the [following YARA rules](#). We will continue to disclose information as it becomes available.

References

- <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>
- <https://tanzu.vmware.com/security/cve-2022-22965>
- <https://www.lunasec.io/docs/blog/spring-rce-vulnerabilities/>
- <https://www.springcloud.io/post/2022-03/spring-0day-vulnerability/>
- https://github.com/Neo23x0/signature-base/blob/master/yara/expl_spring4shell.yar

Version History

Version 3.



Contact Us

24x7 SOC Phone: 215.867.9051

Email: soc@sra.io

Website: <https://sra.io>