SecurityRisk ADVISORS

Threat Bulletin

Spring4Shell

Executive Summary

Wednesday, March 30th: Today an **unconfirmed** zero-day vulnerability called 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.

This vulnerability requires the following Java packages.

- JDK9 and above
- Using the Spring-beans package
- Spring parameter binding is used
- Spring parameter binding uses non-basic parameter types, such as general POJOs

Safeguards/Recommendations

We recommend organizations implement the following YARA rules. We will continue to disclose information as it becomes available.

References

- https://bugalert.org/content/notices/2022-03-30-spring.html
- https://github.com/Neo23x0/signature-base/blob/master/yara/expl_spring4shell.yar

Version History

Version 1. Initial Report

Vendor: Java Spring Framework

CVE-ID: TBD

Published: 03/30/2022

CVSS V3 Overall score: TBD

Criticality: TBD

Patch Availability: TBD

Vulnerability Type: TBD

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

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io