Software AG Security Advisory

Spring Framework RCE vulnerabilities

Announced: Apr-2022 (***Last updated:*** *07-Apr-2022)*

Affects: The Spring RCE (Remote Code Execution) vulnerabilities associated with the Spring Framework library got unfolded during end of March 2022. There are two critical CVEs released for these vulnerabilities.

Some of the Software AG products are impacted by CVE-2022-22965 (Spring4Shell vulnerability) and not impacted by CVE-2022-22963. For the list of impacted products and remediations refer to the 'Impact' section of this document.

Severity: Critical

I. Description

On March 31, 2022, vulnerabilities in the Spring Framework for Java were publicly disclosed. The issue was first reported to VMware late on Tuesday evening (29th March), close to Midnight, GMT time by codeplutos, meizjm3i of AntGroup FG. Vmware worked through investigation, analysis, and is currently identifying a fix, which was released on Thursday 31st March.

The Spring Framework is one of the most widely used lightweight open-source framework for Java. In Java Development Kit (JDK) version 9.0 or later, a remote attacker can obtain an *AccessLogValve* object through the framework's parameter binding feature and use malicious field values to trigger the pipeline mechanism and write to a file in an arbitrary path, if certain conditions are met.

The vulnerability impacts Spring MVC and Spring WebFlux applications running on JDK 9+. 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. Refer to the Am I impacted section on the official Spring website for more information.

Here is the list of vulnerabilities released recently in Spring Framework:

- CVE-2022-22965 (CVSS severity: Critical) - A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.
- CVE-2022-22963 (CVSS severity: Critical) - Remote code execution in Spring Cloud Function by malicious Spring Expression

As soon as the vulnerability information was leaked our security team and product teams proactively worked to release the mitigation/ workaround steps for each product to curb the vulnerability as well as started the work for official fixes. Refer to the 'Workaround' and 'Fix' sections for relevant information impacted product-wise.

Note: This document will be updated if there are more updates to the fixes and mitigations for the above-mentioned vulnerabilities

References:

Spring Framework RCE, Early Announcement

SpringShell: Spring Core RCE 0-day Vulnerability

Spring4Shell Details and Exploit Analysis

II. Impact

Software AG did perform an assessment of the impact on Software AG products associated with these vulnerabilities and created published an announcement on the 'Current Events and Announcements' page in Empower site.

Regarding *CVE-2022-22965*, the impact to Software AG products depends on the specific conditions that are required for the exploit:

- Running on JDK 9 or higher
- Apache Tomcat as the Servlet container.
- Packaged as a traditional WAR and deployed in a standalone Tomcat instance. Typical Spring Boot deployments using an embedded Servlet container or reactive web server are not impacted.
- spring-webmvc or spring-webflux dependency.
- Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions.

Our teams have performed the assessments and published their findings on the impacted product list as part of the respective KB article for each business line.

Regarding *CVE-2022-22963*, our products don't use Spring Cloud Function and are hence not impacted by this vulnerability.

III. Mitigation steps

Mitigation steps for impacted products are listed in the Knowledge Base (KB) articles for each impacted product line. Remember, the mitigation steps are available only if it is applicable. If not available, then the customer must apply the product fix to protect their system. Refer to the KB articles given below for information on impacted products, mitigations, and product fixes. Please note that you will need your Empower credentials to access the following links.

- Adabas
- ARIS
- Cumulocity IoT
- Natural
- webMethods
- webMethods JIS/JI

The necessary information about the fixes can be seen in the Product Fixes section in Empower https://empower.softwareag.com/KnowledgeCenter/Product_Fixes/default.aspx

To get the Early warning updates please subscribe to it in Empower – https://empower.softwareag.com/Preferences/ManageMySubscriptions/earlywarnings.aspx

IV. Contacting Us

If you have questions about this alert or need to report an additional issue, do send an email to Software AG security team:

email : [security@softwareag.com|mailto:security@softwareag.com]

You can reach out to Software AG Global Support either by telephone or by submitting a support incident via the Empower Support Portal.

Or you can also participate in our Software AG Developer Communities, which feature technical information, useful resources, and online discussion forums, moderated by Software AG professionals, to help you do more with technology:

https://empower.softwareag.com/Communities/default.aspx

V. Copyright

Copyright (c) 2022 by Software AG. Permission is granted for copying and circulating this bulletin to Software AG customers for the purpose of alerting them to those topics covered by this bulletin, if and only if, this bulletin is not edited or changed in any way, is attributed

to Software AG and provided such reproduction and/or distribution is performed for non-commercial purposes. Any other use of this information is prohibited.