

Spring Framework: Critical Vulnerability Spring4Shell

<https://campus.barracuda.com/doc/96770693/>

This article provides updates on recently discovered vulnerabilities (CVE-2022-22963 and CVE-2022-22965) in Spring Framework.

The following table provides key information about the vulnerabilities.

CVE Number	Commonly Known/Associated As	Criticality & CVSS Score	Exploit Type	Software Firmware Versions	Prerequisite to Exploit Vulnerability	Barracuda WAF-as-a-Service Affected
CVE-2022-22965	Spring4Shell Relates to old CVE-2010-1622	Zero-day	RCE	Spring MVC and Spring WebFlux applications running on JDK 9+	Application running on Tomcat as the Servlet container	NO
CVE-2022-22963	SpEL (Spring Expression Language)	Critical	ELV->RCE	Spring Cloud Function versions : 3.1.6, 3.2.2 and older unsupported versions		NO

Description

Spring Framework is an application framework and inversion of control container for the Java platform. Recently, two vulnerabilities were discovered in Spring Framework (CVE-2022-22965) and in Spring Cloud Function (CVE-2022-22963).

Spring4Shell is a misnomer for all these vulnerabilities combined (CVE-2022-22965, CVE-2022-22950 & CVE-2022-22963) . Spring4Shell refers to CVE-2022-22965. Also, note that Spring4Shell has no relation with the log4shell vulnerability.

The following sections list the difference between these vulnerabilities, along with their affects and mitigation.

CVE-2022-22963

Description

CVE-2022-22963 was reported on March 29, 2022 - It affects Spring Cloud functions only, which is not

in Spring Framework. Spring has already released a newer version to take care of this. CVE-2022-22963 uses routing functionality to provide specially crafted Spring Expression Language (SpEL) as a routing expression to access local resources and perform RCE. It uses a specific HTTP request header: `spring.cloud.function.routing-expression`.

Barracuda WAF-as-a-Service is not affected by this vulnerability.

Exploit

This is an RCE, and a malicious actor can provide a specially crafted SpEL as a routing expression that may result in access to local resources.

Mitigations

- Barracuda WAF-as-a-Service already mitigates this vulnerability

Recommendation

You can update your infrastructure as follows:

- Vendor Advisory : <https://tanzu.vmware.com/security/cve-2022-22963>
- Users of affected versions should upgrade to 3.1.7, 3.2.3. No other steps are necessary. Releases that have fixed this issue include:
- Spring Cloud Function
 - 3.1.7
 - 3.2.3

CVE-2022-22965

Description

This vulnerability affects Spring MVC and Spring WebFlux applications running on JDK 9+. The specific exploit requires the application to run on Tomcat as a WAR deployment and will not work if the Spring Boot executable is in jar deployment. So by default, the deployed application is not vulnerable to this exploit.

Barracuda WAF-as-a-Service is not affected by this vulnerability.

Exploit:

This is an RCE vulnerability, in Spring Core version 5.3.17 or earlier (for 5.3.x) and version 5.2.19 or earlier (for 5.2.x). It appears to be a bypass of protections set up for CVE-2010-1622.

Mitigations:

- Barracuda WAF-as-a-Service already mitigates this vulnerability.

Recommendations:

You can update your infrastructure as follows:

Vendor advisory : <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>

- Spring Framework 5.3.18 and 5.2.20, which contain the fixes, have been released.
- Spring Boot 2.6.6 and 2.5.12 that depend on Spring Framework 5.3.18 have been released.
- Apache Tomcat has released versions 10.0.20, 9.0.62, and 8.5.78 which close the attack vector on Tomcat's side, see Spring Framework RCE, Mitigation Alternative.

Further Reading:

- <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>
- <https://spring.io/blog/2022/>
- <https://thehackernews.com/2022/03/security-patch-releases-for-critical.html>
- <https://securityboulevard.com/2022/04/critical-alert-spring4shell-rce-cve-2022-22965-in-spring/>
- <https://www.databreachtoday.com/springshell-spring-cloud-function-bugs-need-urgent-patching>
= [a-18822?rf=2022-04-01_ENEWS_ACQ_DBT_Slot1_ART18822&mkt_tok=MDUxLVpYSS0yMzcAAAGDhN0UVdOzrHrKZ5NyWSdphDsc9RZujJR2Ql6F_wl1E76Mg_Jl9Kwj1UwpdfwvOvnl_wfRLxm9p9ZCw5fXY2mVj8IKo2bgINjkzUq4o191m9OkRoKzMQ](https://www.databreachtoday.com/springshell-spring-cloud-function-bugs-need-urgent-patching)

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.