Security Advisory 2022-023

Critical RCE Vulnerability in Spring Core

April 5, 2022 — v1.2

TLP:WHITE

History:

- *31/03/2022 — v1.0 – Initial publication*
- *31/03/2022 — v1.1 – Update with info about the patch*
- *05/04/2022 — v1.2 – Update with VMware Security patch*

Summary

On 29/03/2022, some cybersecurity analysts were alarmed following the publication of a few posts from a Chinese Twitter account. These tweets contained screenshots showing a 0-day exploit in Spring Core, a popular Java library.

The vulnerability has been assigned `CVE-2022-22965` [6, 7], and it is being referred to as `Spring4Shell` [2, 4]. The key points known at this time are:

- This vulnerability allows an unauthenticated attacker to execute arbitrary code on the targeted system.
- Proofs-of-Concept (PoCs) of this vulnerability are **publicly** available.
- **Patches have been released.**

CERT-EU recommends to patch as soon as possible.

Additionally, another Spring vulnerability was also part of the recent discussions on the internet - assigned CVE number `CVE-2022-22963` (CVSS score 9.0) [1], it is a remote code execution vulnerability in Spring Cloud Function, which is a separate Java library from Spring Core. Public POCs are available [1]. CERT-EU recommend to also patch this vulnerability as soon as possible.

Technical Details

Spring4Shell (`CVE-2022-22965`)

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 [6].

The exploitation of this vulnerability requires an endpoint with *DataBinder* enabled (e.g., a POST request that decodes data from the request body automatically) and depends heavily on the servlet container for the application. *For example, when Spring is deployed to Apache Tomcat, the `WebAppClassLoader` is accessible, which allows an attacker to call getters and setters to ultimately write a malicious JSP file to disk. However, if Spring is deployed using the Embedded Tomcat Servlet Container the classloader is a `LaunchedURLClassLoader` which has limited access* [2].

Affected Products

Specific requirements seem to be needed to be directly affected by `CVE-2022-22965` (Spring4Shell):

- JDK 9 or higher
- Apache Tomcat as the Servlet container
- Packaged as WAR
- `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

Additionnaly, VMware has published security updates about its cloud computing and virtualization products that are impacted by this vulnerability [3]:

- VMware Tanzu Application Service for VMs – versions 2.10 to 2.13
- VMware Tanzu Operations Manager – versions 2.8 to 2.10
- VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) – versions 1.11 to 1.13

Regarding the `CVE-2022-22963` :

- Spring Cloud Function
  - 3.1.6
  - 3.2.2
  - Older, unsupported versions are also affected.

Recommendations and Workarounds

Spring Framework versions 5.3.18 and 5.2.20, which address the `CVE-2022-22963` vulnerability, are now available on Maven Central. Spring Boot 2.5.12 with Spring Framework 5.3.18 and 5.3.20 is also available [6]. It is strongly recommended to upgrade as soon as possible.

Regarding VMware products, the vendor has already made available security updates for the first two affected softwares but a permanent fix for VMware Tanzu Kubernetes Grid Integrated Edition is still in the works [3, 8]. Furthermore, VMWare has published workaround instructions designed to help administrators mitigate the issue on their systems until the patches are released [9].

For the `CVE-2022-22963` vulnerability, CERT-EU strongly recommends to upgrade to 3.1.7+ or 3.2.3+ to mitigate this RCE.

Mitigations

If patching of `CVE-2022-22965` is not immediately possible, the recommended approach is to apply the workaround in a more fail-safe way - applications could extend `RequestMappingHandlerAdapter` to update the `WebDataBinder` at the end after all other initialisation [6]. Other (earlier) attempts at the mitigations are also described in [2, 4].

Finally, Randori Attack Team has proposed *non-malicious* request to test the susceptibility for this vulnerability [5].

References

[1] https://sysdig.com/blog/cve-2022-22963-spring-cloud

[2] https://www.praetorian.com/blog/spring-core-jdk9-rce/

[3] https://www.vmware.com/security/advisories/VMSA-2022-0010.html

[4] https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/

[5] https://twitter.com/RandoriAttack/status/1509298490106593283

[6] https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

[7] https://tanzu.vmware.com/security/cve-2022-22965

[8] https://www.bleepingcomputer.com/news/security/vmware-patches-spring4shell-rce-flaw-in-multiple-products/

[9] https://kb.vmware.com/s/article/88102