Spring4shell vulnerability

CVE:

2022–22965

CVSS Score

9.8

Abstract

The Spring framework is the most widely used lightweight open-source framework for Java, and in the JDK9 version of the Spring framework (and above), 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. file under any path.

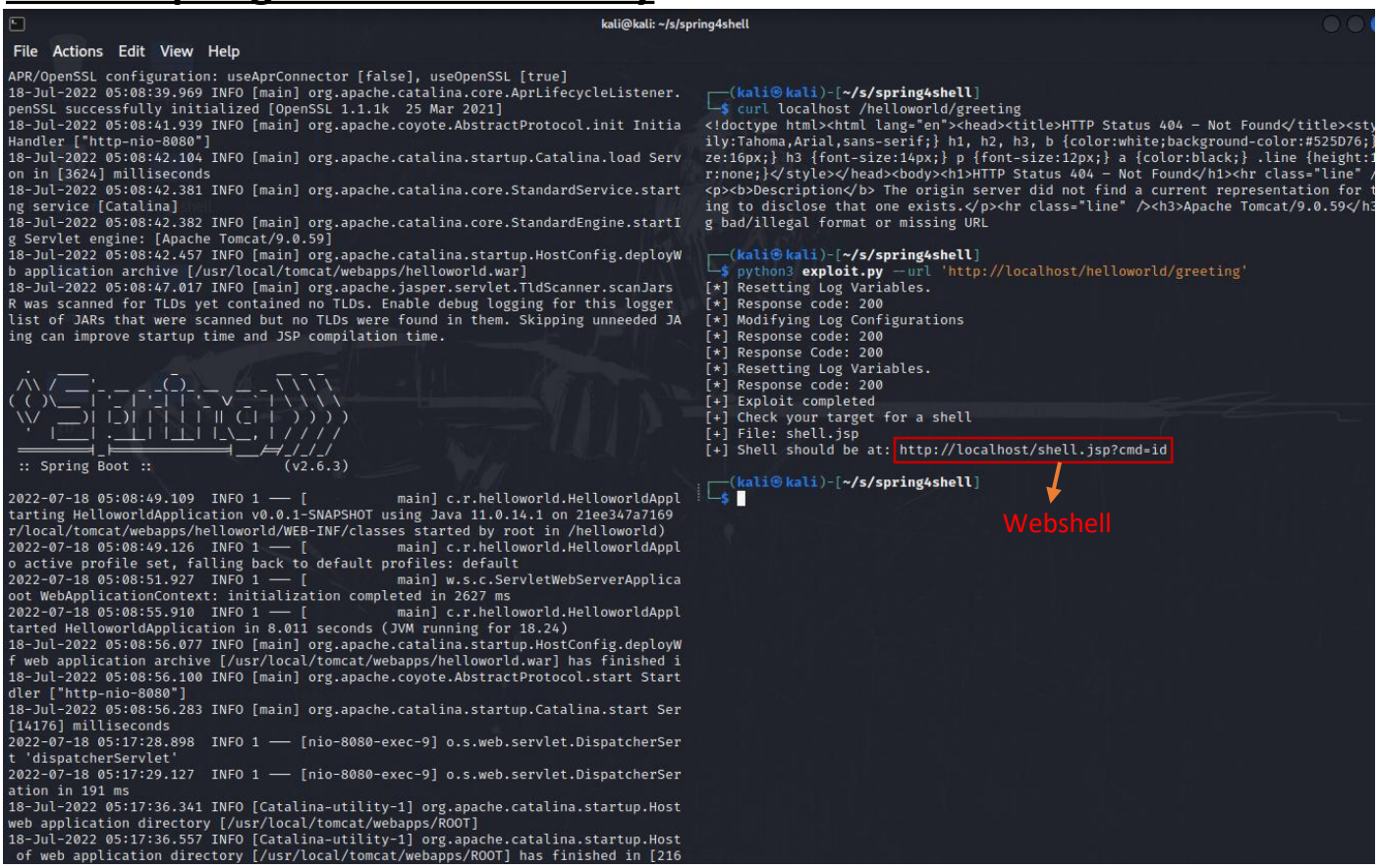
The Spring4Shell vulnerability (CVE-2022–22965) impacts SpringMVC (Spring Web model-view-controller) and Spring WebFlux applications when running on Java JDK9 and subsequently on a Tomcat application server. The vulnerability can be exploited to write to an arbitrary file on the server, which can then be leveraged to achieve remote code execution.

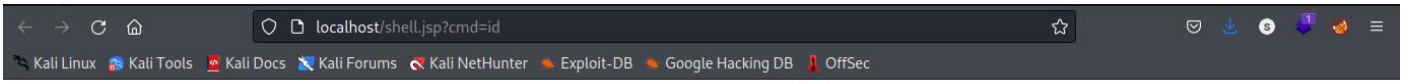
The exploit code that has been made public specifically targets Apache Tomcat deployments. It only affects Spring Applications that are deployed as traditional WebArchive (WAR) files to the Apache Tomcat Servlet container.The main issue occurs when we have a controller that has a request mapping loaded into memory.

Condition for Exploiting the Vulnerability

- JDK 9 or higher
- Apache Tomcat as the Servlet container (A vulnerable Tomcat server with a vulnerable spring4shell application.)
- 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
- Packaged as a traditional WAR (in contrast to a Spring Boot executable jar)

POC of Spring4Shell Vulnerability

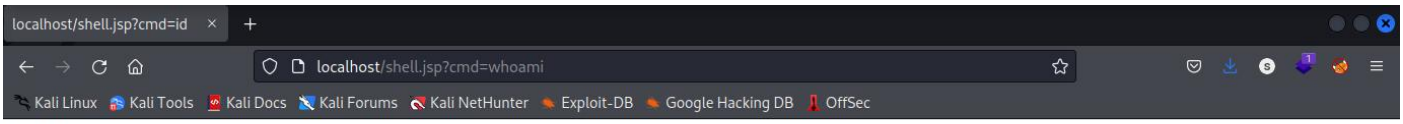




uid=0(root) gid=0(root) groups=0(root) //

Hello World! Exploit me!

total 24K drwxr-xr-x 1 root root 4.0K Jul 18 05:33 . drwxr-xr-x 1 root root 4.0K Jul 18 05:08 .. drwxr-x--- 2 root root 4.0K Jul 18 05:33 exploit -rw-r--r-- 1 root root 1.8K Jul 18 04:55 pom.xml drwxr-xr-x 4 root root 4.0K Jul 18 04:58 src drwxr-xr-x 1 root root 4.0K Jul 18 05:04 target //



root //

Mitgation

- Use of Spring Framework 5.3.18+ & 5.2.20+ is not vulnerable to this Exploit
- The Apache Software Foundation has also released patched versions of Apache Tomcat 10.0.20, 9.0.62, and 8.5.78, in which the attack vector is closed on the Tomcat side.
- The Spring developers have also released patched versions of the Spring Boot 2.5.12 and 2.6.6 extensions that depend on the patched version of Spring Framework 5.3.18.

Lab

https://www.thedutchhacker.com/spring4shell-cve-2022-22965-on-tryhackme/

Reference

- https://infosecwriteups.com/anatomy-of-spring4shell-cve-2022-22965-e0df259cef9d
- https://www.kaspersky.co.in/blog/spring4shell-critical-vulnerability-in-spring-java-framework/24004/
- https://websecured.io/blog/624411cf775ad17d72274d16/spring4shell-poc/