GUIDEPOINT SECURITY

Threat Bulletin: SpringShell Vulnerability Targeting Spring Framework Core Module

GuidePoint Research and Intelligence Team (GRIT)

Summary

On March 30, 2022, a Chinese Security Researcher posted a proof-of-concept (POC) to GitHub documenting a vulnerability discovered in the Spring Framework module, Spring Core. This vulnerability, labeled by members of the information security community as SpringShell or Spring4Shell, has since been confirmed by the Spring Framework developers and published as CVE-2022-22965.

SpringShell Zero-Day Released to GitHub

"On March 30, 2022, a security researcher maintaining the GitHub repository "spring-rce-war" posted a POC targeting the Spring Core module in the Spring Framework, a popular Java framework. Shortly after posting the POC, this researcher deleted the repository." The vulnerability involves an attacker specifying additional parameters in an HTML request which allows the attacker to modify the ClassLoader with classes that were not intended by the application. This manipulation event includes creating a new file in the webapps/ROOT directory and populating it with a web shell. Once created, the attacker simply browses to their newly created web shell and specifies their remote code executions in the URL. The server responds to the attacker with relevant output from the executed command(s). VMware has since confirmed this exploit applies to Spring Framework versions 5.3.0 - 5.3.17, 5.2.0 - 5.2.19, and may affect unsupported and outdated versions of Spring Framework.

Affected Applications

Spring Framework developers advise that there are multiple requirements for an application to be vulnerable to CVE-2022-22965:

- Java Developer Kit 9 or newer
- A Servlet container running on Apache Tomcat
- Application must be run as a WAR deployment
- Application must depend on spring-webmwv and spring-webflux

While these conditions are required for the currently observed exploitation to be successful, these requirements are subject to change if additional methodologies are discovered.

Recommendations

GRIT recommends taking the following actions to patch applications or mitigate risk on vulnerable systems.

Update Spring Framework and Spring Boot

If able, upgrade Spring Framework to versions 5.3.18 or 5.2.20. If Spring Boot is in use, it must also be updated. The updates for Spring Boot to 2.5.12 and 2.6.6 are available.

If upgrading Spring Framework and Spring Boot is not an option, Spring has posted more detailed guidance on mitigating the affected application.

Search for Affected Applications

- For applications deployed via Apache Tomcat as a WAR deployment:
- Decompress .war packages which might rely on Spring
- Search decompressed results for 'spring-beans-*.jar' file
- Search decompressed results for CachedIntrospectionResuLts.class file

If either `spring-beans-*.jar` or `CachedIntrospectionResuLts.class` exist, the application is developed using the Spring Framework and should be updated or mitigation actions should be taken.

Detection Opportunities

The following recommendations may aide in detecting ongoing or future exploitation attempts of the Spring vulnerabilities outlined in this threat bulletin:

- Search for suspicious new files in the webserver directory (particularly web shells)
- In your EDR platform look for suspicious subprocesses of the vulnerable webserver executable (such as powershell.exe, cmd.exe)
- If you have a WAF or other logging enabled hunt for requests that reference `.class` files (`class.*`, `Class.*`, `*.class.*`, and `*.Class.*`)

The following sources are available to aid in the creation of detection capabilities for SpringShell:

signature-base/expl_spring4shell.yar at master · Neo23x0/signature-base (github.com)

Need Help?

If you think you are affected by these Spring vulnerabilities and need assistance, contact GRIT at GRIT@guidepointsecurity.com.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.