BOLETÍN DE ALERTA

Boletín Nro.: 2022-20

Fecha de publicación: 31/03/2022

Tema: Múltiples vulnerabilidades en Java Spring Framework

Las versiones de Java Spring Framework afectadas son:

- Spring Framework versión 5.3.0 hasta la versión 5.3.17;
- Spring Framework versión 5.2.0 hasta la versión 5.2.19;
- Spring Framework versiones más antiguas y sin soporte también se ven afectadas;
- Spring Cloud Function versión 3.1.6 y la versión 3.2.2;
- Spring Cloud Function las versiones más antiguas y sin soporte también se ven afectadas.
- Spring Core, todas las versiones (según diversos investigadores, afecta a todos los usuarios que ejecutan JDK versión 9 y superiores, debido a una corrección parcial de la vulnerabilidad CVE-2010-1622).

Descripción:

Se han detectado múltiples vulnerabilidades en Java Spring Framework que permitirían a un atacante realizar ejecución remota de código (RCE), acceder a los recursos locales de la aplicación afectada y realizar una denegación de servicio (DoS). Las vulnerabilidades se detallan a continuación:

CVE-2022-22950 de severidad media, con una puntuación asignada de 5.4. En esta vulnerabilidad un usuario podría proporcionar una expresión SpEL (*Spring Expression Language*) diseñada especialmente para causar una condición de denegación de servicio (DoS) en *Spring Framework*.

CVE-2022-22963 de severidad crítica, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a que al utilizar la funcionalidad de enrutamiento, un usuario podría proporcionar una expresión SpEL especialmente diseñada como expresión de enrutamiento, que permitiría a un atacante acceder a los recursos locales y ejecutar comandos en el *host* de *Spring Cloud Function*. El parámetro *spring.cloud.function.routing-expression* existe en el encabezado de solicitud HTTP de acceso a *Spring Cloud Function*, y su expresión SpEL se puede inyectar y ejecutar a través de *StandardEvaluationContext*. Esto permitiría a un atacante utilizar esta vulnerabilidad para realizar la ejecución remota de código (RCE).

CVE-2022-22965 de severidad crítica, con una puntuación asignada de 10. Esta vulnerabilidad *Spring4Shell* podría permitir a un atacante remoto no autenticado, ejecutar

código arbitrario en el sistema objetivo a través del enlace de datos. La explotación de esta vulnerabilidad solo requiere que un atacante envíe una solicitud HTTP diseñada a un sistema vulnerable. Sin embargo, la explotación de diferentes configuraciones requerirá que el atacante realice una investigación adicional para encontrar cargas útiles que sean efectivas.

El *exploit* específico requiere que la aplicación se ejecute en Tomcat como una implementación de WAR. Si la aplicación se implementa como un jar ejecutable de Spring Boot, es decir, el predeterminado, no es vulnerable al *exploit*.

Requisitos previos para la explotación de *Spring4Shell*:

- JDK 9 o superior
- Apache Tomcat como contenedor de servlets
- Empaquetado como WAR
- dependencia *spring-webmvc* o *spring-webflux*

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante realizar ejecución remota de código (RCE), acceder a los recursos locales de la aplicación afectada o realizar una denegación de servicio (DoS).

Solución:

Se recomienda descargar e instalar las actualizaciones de los productos afectados proveídas por el fabricante:

- Spring Framework a la versión 5.3.18 o posteriores.
- Spring Cloud Function actualizar a las versiones 3.1.7 y 3.2.3.
- Spring Boot 2.6.6. La versión de Spring Framework en esta versión incluye una solución para CVE-2022-22965.
- Spring Core, como medida de mitigación temporal recogida, se recomienda crear un componente *ControllerAdvice* (que es un componente de Spring compartido entre *Controllers*) y añadir una *blacklist* de patrones de campos vulnerables necesarios para la explotación. Adicionalmente, otras medidas de mitigación para *Spring4Shell* son:
  - implementar reglas de filtrado y monitorización en el WAF, haciendo referencia a "class" ("class.*", "*.class.*", "Class.*", y "*.Class.*");
  - utilizar reglas de Yara para detectar actividades relacionadas.

Información adicional:

- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-spring

- https://www.securityweek.com/spring4shell-spring-flaws-lead-confusion-concerns-new-log4shell-threat
- https://www.cyberkendra.com/2022/03/rce-0-day-exploit-found-in-spring-cloud.html
- https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-code.html
- https://tanzu.vmware.com/security/cve-2022-22950
- https://tanzu.vmware.com/security/cve-2022-22963
- https://nvd.nist.gov/vuln/detail/CVE-2010-1622
- https://thehackernews.com/2022/03/unpatched-java-spring-framework-0-day.html
- https://spring.io/blog/2022/03/29/cve-report-published-for-spring-cloud-function
- https://threatpost.com/critical-rce-bug-spring-log4shell/179173/
- https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-vulnerability-in-spring-framework/