BOLETÍN DE ALERTA

Boletín Nro.: 2023-22
Fecha de publicación: 19/05/2023
Tema: Vulnerabilidades críticas en Spring Boot framework de Java.

El software afectado es:

- Spring Boot, versiones 3.0.0 a 3.0.6.
- Spring Boot, versiones 2.7.0 a 2.7.11
- Spring Boot, versiones 2.6.0 a 2.6.14.
- Spring Boot, versiones 2.5.0 a 2.5.14
- Versiones anteriores que ya no cuentan con soporte.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre dos vulnerabilidades que afectan al framework de desarrollo para Java llamado Spring Boot, que permitirían a un atacante realizar omisión de seguridad y denegación de servicios (*DoS*) en el sistema afectado.

- CVE-2023-20873, de severidad "Crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad de omisión de seguridad se debe a una falla en la gestión de solicitudes que coinciden con el comodín */cloudfoundryapplication/**/** en Cloud Foundry de Spring Boot. Esto permitiría a un atacante remoto a través de la utilización de patrones de coincidencia y la implementación de aplicaciones en Cloud Foundry, realizar evasión de controles de seguridad en el sistema afectado. Recientemente hemos publicado una noticia con información de dicha vulnerabilidad aquí.

- CVE-2023-20883, de severidad "Alta", sin puntuación asignada aún. Esta vulnerabilidad se debe a una falla de seguridad al utilizar *Spring MVC* con una caché de *proxy* inverso en Spring Boot. La aplicación es vulnerable solo si posee la configuración automática de *Spring MVC* habilitada. Esto permitiría a un atacante a través de la configuración de un *proxy* almacenado en caché, provocar ataques de denegación de servicios (*DoS*) en el sistema afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar omisión (bypass) de seguridad y denegación de servicios (*DoS*) en el sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en los siguientes enlaces:

- Spring Boot v3.0.7.
- Spring Boot v2.7.12.
- Spring Boot v2.6.15.
- Spring Boot v2.5.15.

Mitigación:

Adicionalmente, como medida de mitigación para la vulnerabilidad CVE-2023-20883 se recomienda tener en cuenta los siguientes pasos:

- Configurar el *proxy* inverso para que no almacene en caché las respuestas HTTP 404.
- Deshabilitar el *actuator endpoints* de Cloud Foundry estableciendo el parámetro *management.cloudfoundry.enabled* en *false*.

Información adicional:

- https://securityonline.info/cve-2023-20883-cve-2023-20873-two-high-severity-vulnerabilities-in-spring-boot/
- https://nvd.nist.gov/vuln/detail/CVE-2023-20873
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20883
- https://spring.io/security/cve-2023-20873
- https://spring.io/security/cve-2023-20883
- https://github.com/spring-projects/spring-boot/releases
- https://www.cert.gov.py/noticias/vulnerabilidad-de-evasion-de-controles-de-seguridad-en-spring-boot/
- Release v3.0.7 · spring-projects/spring-boot · GitHub
- Release v2.7.12 · spring-projects/spring-boot · GitHub
- Release v2.6.15 · spring-projects/spring-boot · GitHub
- Release v2.5.15 · spring-projects/spring-boot · GitHub