BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-56
Fecha de publicación: 21/10/2024
Tema: Vulnerabilidad Crítica en Spring Framework
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Spring Framework
  - 5.3.0 hasta 5.3.40
  - 6.0.0 hasta 6.0.24
  - 6.1.0 hasta 6.1.13

Descripción

Se ha identificado una nueva vulnerabilidad crítica de path traversal **Spring Framework**, identificada como **CVE-2024-38819**. Esta vulnerabilidad afecta varias versiones de este framework, el cual es utilizado comúnmente en aplicaciones web basadas en Java. Esta vulnerabilidad permite a un atacante manipular las rutas de archivos dentro de una aplicación web para acceder a archivos fuera del directorio permitido. En este caso, la vulnerabilidad afecta a las aplicaciones que utilizan los marcos funcionales **WebMvc.fn** o **WebFlux.fn** para servir recursos estáticos.

La explotación ocurre cuando un atacante envía solicitudes HTTP maliciosas que manipulan las rutas de los archivos estáticos solicitados. Si no se manejan adecuadamente las rutas de los archivos en la aplicación, el atacante puede navegar hacia directorios críticos del sistema y acceder a archivos que están accesibles para el proceso que ejecuta la aplicación Spring.

Con más de **2000 aplicaciones** utilizando **Spring Framework en México**, la presencia de esta plataforma en entornos de desarrollo web es significativa, por ello la urgencia de corregir esta vulnerabilidad y evitar consecuencias graves para la confidencialidad e integridad de los datos alojados en servidores locales.

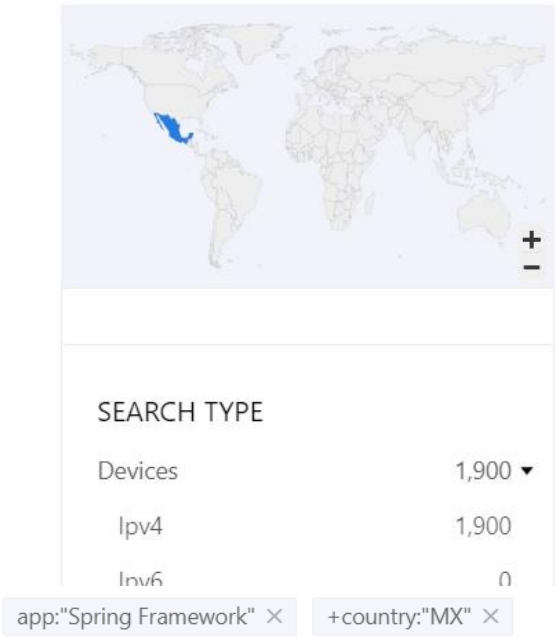

Imagen Total de apps con Spring Framework en México (https //zoomeye.hk)

Solución

Es fundamental actualizar a las versiones corregidas (5.3.41, 6.0.25 y 6.1.14) para mitigar este riesgo. Las aplicaciones que no puedan actualizarse inmediatamente pueden implementar medidas de mitigación temporales, como el uso del **Spring Security HTTP Firewall** o la migración a servidores como **Tomcat** o **Jetty**, que bloquean las solicitudes maliciosas.

Puedes encontrar más información y detalles sobre los parches de seguridad vista el siguiente enlace https://enterprise.spring.io

Información adicional:

- https://securityonline.info/spring-framework-vulnerability-cve-2024-38819-path-traversal-risk-in-web-apps/?&web_view=true
- https://spring.io/blog/2024/10/17/spring-framework-cve-2024-38819-and-cve-2024-38820-published
- https://medium.com/@patchnow/cve-2024-38819-path-transversal-vulnerability-in-spring-framework-c7e04ab0a16f

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com