La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó el lunes la vulnerabilidad de ejecución remota de código (RCE) recientemente revelada, que afecta a Spring Framework, a su Catálogo de Vulnerabilidades Explotadas Conocidas basado en *«evidencia de explotación activa».*

La vulnerabilidad de gravedad crítica tiene el identificador CVE-2022-22965, con puntuación CVSS de 9.8, y se denominó Spring4Shell, afecta a las aplicaciones Spring model-view-controller (MVC) y Spring WebFlux, que se ejecutan en Java Development Kit 9 y versiones posteriores.

> *«La explotación requiere un punto final con DataBinder habilitado (por ejemplo, una solicitud POST que decodifica los datos del cuerpo de la solicitud automáticamente), y depende en gran medida del contenedor de servlet para la aplicación»,* dijeron los investigadores de Praetorian, Anthony Weems y Dallas Kaman.

Aunque los detalles exactos del abuso en estado salvaje siguen sin estar claros, la compañía de seguridad de la información SecurityScorecard, dijo que *«se ha observado un escaneo activo de esta vulnerabilidad proveniente de los sospechosos habituales, como el espacio IP ruo y chino».*

Akamai y Unit42 de Palo Alto Networks, detectaron actividades de escaneo similares, y los intentos llevaron a una implementación de un shell web para acceso de puerta trasera y para ejecutar comandos arbitrarios en el servidor con el objetivo de entregar otro malware o propagarse dentro de la red de destino.

> *«Durante los primeros cuatro días posteriores al brote de la vulnerabilidad, el 16% de las organizaciones en todo el mundo se vieron afectadas por intentos de explotación»,* dijo CheckPoint Research, agregando que detectó 37,000 ataques relacionados con Spring4Shell durante el fin de semana.

El equipo de inteligencia de amenazas de Microsoft 365 Defender también intervino, diciendo que estuvo *«rastreando un bajo volumen de intentos de explotación en nuestros servicios en la nube para las vulnerabilidades de Spring Cloud y Spring Core».*

Según las estadísticas publicadas por Sonartype, las versiones potencialmente vulnerables de Spring Framework representan el 81% del total de descargas del repositorio de Maven Central desde que el problema se informó públicamente el 31 de marzo.

Cisco, que está investigando activamente su línea para determinar cuál de sus equipos puede verse afectado por la vulnerabilidad, confirmó que tres de sus productos están siendo afectados:

- Motor de optimización de Cisco Crosswork
- Cisco Crosswork Zero Touch Provisioning (ZTP)
- Intelitencia permitetral de Cisco

VMware, por su parte, también consideró que tres de sus productos son vulnerables y ofrecerá parches y soluciones:

- Servicio de aplicaciones VMware Tanzu para máquinas virtuales
- Gerente de operaciones de VMware Tanzu
- Filial de VMware Kubernetes Grid Integrated Edition (TKGI)

> *«Un actor malicioso con acceso a la red de un producto de VMware afectado puede explotar este problema para obtener el control total del sistema de destino»,* dijo VMware.

CISA también agregó a su catálogo dos vulnerabilidades de día cero parcheadas por Apple la semana pasada (CVE-2022-22674 y CVE-2022-22675) y una deficiencia crítica en los routers D-Link (CVE-2021-45382) que ha sido activamente armado por la campaña DDoS basada en Beastmode Mirai.

Según la conformidad con la Directiva Operativa Vinculante (BOD) emitida por CISA en noviembre de 2021, las agencias del Poder Ejecutivo Civil Federal (FCEB) deben corregir las vulnerabilidades identificadas antes del 25 de abril de 2022.