BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-49
Fecha de publicación: 10/10/2024
Tema: Vulnerabilidad Crítica de Ejecución Remota de Código en Productos Fortinet
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- FortiOS: versiones anteriores a la 7.0.12 y 7.2.5
- FortiProxy: versiones anteriores a la 7.0.9 y 7.2.3
- FortiWeb: versiones anteriores a la 6.3.19

Descripción

CISA ha alertado sobre la explotación activa de una vulnerabilidad crítica de **ejecución remota de código (RCE)** en productos de **Fortinet**, identificada como **CVE-2024-23113**. Esta vulnerabilidad afecta a varias soluciones de Fortinet, incluidas **FortiOS**, **FortiPAM**, **FortiProxy**, y **FortiWeb**.

La falla se debe a un problema de **cadena de formato** en el daemon **fgfmd** de FortiOS, que podría permitir a un atacante remoto y no autenticado ejecutar comandos o código arbitrario en el sistema afectado mediante solicitudes manipuladas. La gravedad de la vulnerabilidad se refleja en su puntuación CVSS de **9.8**, calificándola como crítica.

Según datos de Shodan, en México se cuentan con más de **15 mil dispositivos** Fortinet activos proporcionando diversas capas de seguridad en redes y aplicaciones como lo son **FortiOS,** que es el sistema operativo que gestiona los cortafuegos; FortiGate, controlando el tráfico de red y protegiendo contra amenazas. **FortiProxy** que actúa como un proxy seguro para gestionar y filtrar el tráfico web, defendiendo a las organizaciones de amenazas en línea y **FortiWeb,** que es un firewall especializado en proteger aplicaciones web y sitios contra ataques como inyecciones SQL y XSS, asegurando la integridad de las aplicaciones.

Imagen Dispositivos Fortinet en México

Solución

Para mitigar la vulnerabilidad **CVE-2024-23113** en los productos de Fortinet, la solución es **actualizar a las versiones parcheadas**. Fortinet ha lanzado actualizaciones que corrigen esta vulnerabilidad. Para mas información visita el siguiente link: https://support.fortinet.com/

Información adicional:

- https://www.bleepingcomputer.com/news/security/cisa-says-critical-fortinet-rce-flaw-now-exploited-in-attacks
- https://thehackernews.com/2024/10/cisa-warns-of-critical-fortinet-flaw-as.html
- https://www.theregister.com/2024/10/10/cisa_ivanti_fortinet_vulns/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com