Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET BAJO ATAQUE: VULNERABILIDAD CRÍTICA CVE-2024-23113 ACTIVA EN FORTIOS

10 / 10 / 2024

CONTENIDO

INTRODUCCIÓN

CISA ha emitido una alerta urgente sobre la explotación activa de una vulnerabilidad crítica (CVE-2024-23113) en dispositivos Fortinet, que permite a cibercriminales ejecutar código remotamente sin interacción del usuario. Este fallo afecta a varias versiones de FortiOS, FortiPAM, FortiProxy y FortiWeb, poniendo en riesgo a organizaciones que aún no han aplicado los parches de seguridad correspondientes. La vulnerabilidad, de baja complejidad, puede ser utilizada para comprometer dispositivos desactualizados, lo que subraya la importancia de mantener los sistemas actualizados y seguir las recomendaciones de seguridad emitidas por CISA.

FORTINET BAJO ATAQUE: VULNERABILIDAD CRÍTICA CVE-2024-23113 ACTIVA EN FORTIOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_10_10_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/10/2024
Es día cero (0 day):	No

RESUMEN

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha emitido una advertencia urgente a administradores de redes y usuarios de Fortinet: la vulnerabilidad crítica CVE-2024-23113 está siendo activamente explotada por actores maliciosos.

La vulnerabilidad, descubierta en el Daemon de FortiOS, permite la ejecución remota de código (RCE) sin necesidad de interacción del usuario, lo que facilita ataques de baja complejidad. Este fallo se presenta en varios productos de Fortinet, incluidos FortiOS 7.0 y versiones posteriores, FortiPAM, FortiProxy y FortiWeb.

El Daemon vulnerable, encargado de gestionar las solicitudes de autenticación y otros procesos clave, puede ser explotado por actores no autenticados para ejecutar comandos maliciosos o tomar el control de dispositivos que no han sido parcheados.

Impacto y productos afectados

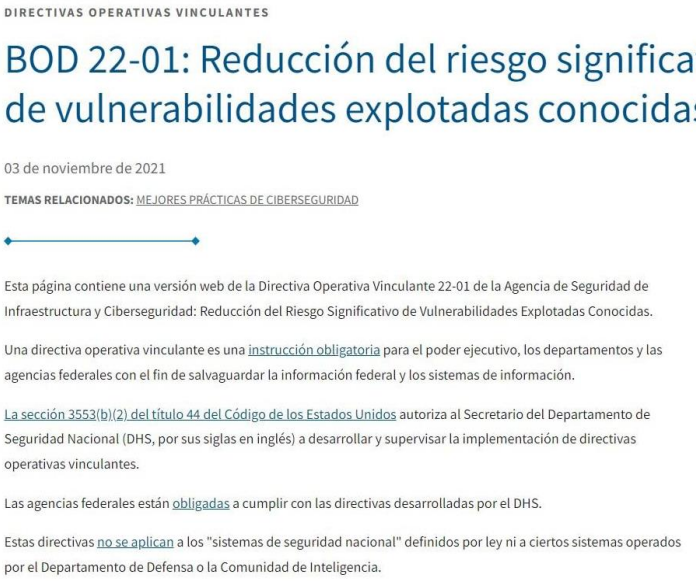
Los productos afectados incluyen:

- FortiOS 7.0 y versiones posteriores
- FortiPAM 1.0 y superiores
- FortiProxy 7.0 y versiones más recientes
- FortiWeb 7.4

Fortinet ya había divulgado y parcheado este fallo en febrero de 2024, pero muchos sistemas aún permanecen sin actualizar, lo que aumenta el riesgo de ser víctimas de ataques.

Medidas tomadas por CISA

A raíz de la explotación activa, CISA ha añadido esta vulnerabilidad a su catálogo de vulnerabilidades explotadas. Las agencias federales de EE. UU. tienen hasta el 30 de octubre para parchear los dispositivos FortiOS en sus redes, siguiendo el mandato operativo BOD 22-01.



DIRECTIVAS OPERATIVAS VINCULANTES

BOD 22-01: Reducción del riesgo significativo de vulnerabilidades explotadas conocidas

03 de noviembre de 2021

TEMAS RELACIONADOS: MEJORES PRÁCTICAS DE CIBERSEGURIDAD

Esta página contiene una versión web de la Directiva Operativa Vinculante 22-01 de la Agencia de Seguridad de Infraestructura y Ciberseguridad: Reducción del Riesgo Significativo de Vulnerabilidades Explotadas Conocidas.

Una directiva operativa vinculante es una instrucción obligatoria para el poder ejecutivo, los departamentos y las agencias federales con el fin de salvaguardar la información federal y los sistemas de información.

La sección 3553(b)(2) del título 44 del Código de los Estados Unidos autoriza al Secretario del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) a desarrollar y supervisar la implementación de directivas operativas vinculantes.

Las agencias federales están obligadas a cumplir con las directivas desarrolladas por el DHS.

Estas directivas no se aplican a los "sistemas de seguridad nacional" definidos por ley ni a ciertos sistemas operados por el Departamento de Defensa o la Comunidad de Inteligencia.

CISA subraya que esta vulnerabilidad representa un riesgo significativo, ya que las vulnerabilidades RCE son frecuentemente utilizadas por actores cibercriminales para comprometer redes empresariales.

Recomendaciones de CISA

CISA recomienda las siguientes acciones urgentes para mitigar esta amenaza:

1. Aplicar los parches: Asegúrese de que sus dispositivos Fortinet estén actualizados con los parches más recientes publicados por la empresa en febrero.
2. Limitar el acceso: Restringir el acceso al Daemon FGFMD para reducir la superficie de ataque. Aunque esta medida no elimina por completo la vulnerabilidad, es un paso esencial para mitigar los riesgos.
3. Implementar políticas de acceso local: Configure una política local que permita conexiones FGFM solo desde IP específicas para limitar posibles puntos de acceso.

Recordatorio para los administradores

Este incidente es un recordatorio crucial para todos los administradores de redes: mantener los dispositivos actualizados y aplicar los parches de seguridad de forma oportuna es esencial para protegerse contra ataques cibernéticos. Las vulnerabilidades no corregidas son una puerta de entrada fácil para los cibercriminales, que pueden aprovechar cualquier descuido en la seguridad para comprometer redes enteras.

Conclusión

La explotación activa de la vulnerabilidad CVE-2024-23113 es una llamada de atención para todos los usuarios de Fortinet. Asegurarse de tener los sistemas actualizados y seguir las recomendaciones de CISA es vital para reducir el riesgo de ciberataques que pueden comprometer la integridad de su infraestructura.

Mantente alerta, actualiza tus sistemas y refuerza tus medidas de seguridad hoy mismo.

NOTICIA COMPLETA

https://devel.group/blog/fortinet-bajo-ataque-vulnerabilidad-critica-cve-2024-23113-activa-en-fortios/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/blog