Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVO FALLO CRÍTICO EN FORTIOS SSL VPN PODRÍA ESTAR SIENDO EXPLOTADO EN

09 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

En medio del panorama de ciberseguridad actual, Fortinet ha emitido una advertencia crítica sobre una nueva vulnerabilidad en su producto estrella, FortiOS SSL VPN. Esta vulnerabilidad, identificada como CVE-2024-21762, ha sido clasificada con una gravedad de 9.6 y permite a atacantes no autenticados ejecutar código de forma remota. Aunque no se han proporcionado detalles sobre la explotación de esta vulnerabilidad ni sobre su descubrimiento, la recomendación de Fortinet es clara: actualizar a las últimas versiones disponibles o, para aquellos que no puedan aplicar parches de inmediato, deshabilitar SSL VPN como medida de mitigación. En un contexto donde las amenazas cibernéticas son cada vez más sofisticadas, este nuevo fallo representa una seria preocupación, especialmente dado el historial de ataques dirigidos a dispositivos Fortinet. La actualización oportuna de los sistemas se vuelve crucial para protegerse contra posibles exploits y salvaguardar la integridad de las redes corporativas frente a amenazas cada vez más persistentes.

NUEVO FALLO CRÍTICO EN FORTIOS SSL VPN PODRÍA ESTAR SIENDO EXPLOTADO EN ATAQUES

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

ID de alerta:	DSOC-CERT_2024_02_09_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/02/2024
Es día cero (0 day):	No

RESUMEN

Fortinet ha emitido una advertencia sobre una nueva vulnerabilidad crítica de ejecución remota de código (RCE, por sus siglas en inglés) en FortiOS SSL VPN que posiblemente esté siendo explotada en ataques.

La vulnerabilidad (identificada como CVE-2024-21762 / FG-IR-24-015) ha recibido una calificación de gravedad de 9.6 y es una vulnerabilidad de escritura fuera de límites en FortiOS que permite a atacantes no autenticados obtener ejecución remota de código a través de solicitudes maliciosamente diseñadas.

Para corregir el error, Fortinet recomienda actualizar a una de las últimas versiones según esta tabla:

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

Para aquellos que no puedan aplicar parches, pueden mitigar la vulnerabilidad deshabilitando SSL VPN en sus dispositivos FortiOS.

El aviso de Fortinet no proporciona detalles sobre cómo se está explotando la vulnerabilidad ni quién descubrió la vulnerabilidad.

Este fallo se reveló hoy junto con CVE-2024-23113 (CVSS de 9.8), CVE-2023-4448 y CVE-2023-47537. Sin embargo, no se indica que estas vulnerabilidades estén siendo explotadas en la naturaleza.

Los actores de amenazas suelen apuntar a fallos de Fortinet para infiltrarse en redes corporativas en ataques de ransomware y espionaje cibernético.

Ayer, Fortinet reveló que actores de amenazas patrocinados por el estado chino, conocidos como Volt Typhoon, dirigieron vulnerabilidades de FortiOS para desplegar malware personalizado conocido como COATHANGER.

Este malware es un troyano de acceso remoto personalizado (RAT, por sus siglas en inglés) diseñado para infectar dispositivos de seguridad de red Fortigate y recientemente se encontró en ataques contra el Ministerio de Defensa holandés.

Debido a la alta gravedad del fallo recién revelado CVE-2024-21762 y la probabilidad de que esté siendo explotado en ataques, se recomienda encarecidamente que actualice sus dispositivos lo antes posible.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240209_1_VoltTyphoon

NOTICIA COMPLETA

https://devel.group/blog/nuevo-fallo-critico-en-fortios-ssl-vpn-podria-estar-siendo-explotado-en-ataques/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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/reporta-un-incidente