Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET ALERTA SOBRE UNA NUEVA VULNERABILIDAD CRÍTICA DE EJECUCIÓN REMOTA DE CÓDIGO

14 / 03 / 2024

CONTENIDO

INTRODUCCIÓN

La seguridad cibernética se encuentra una vez más en el punto de mira con un nuevo aviso emitido por Fortinet. En esta ocasión, la empresa advierte sobre una vulnerabilidad crítica en su software FortiClientEMS, que podría ser explotada por ciberdelincuentes para llevar a cabo ataques de ejecución de código remoto en sistemas vulnerables. Con una calificación de gravedad alarmante, esta noticia destaca la urgencia de tomar medidas proactivas para proteger los activos digitales y la integridad de las organizaciones frente a las amenazas en evolución del panorama cibernético.

FORTINET ALERTA SOBRE UNA NUEVA VULNERABILIDAD CRÍTICA DE EJECUCIÓN REMOTA DE CÓDIGO

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

ID de alerta:	DSOC-CERT_2024_03_14_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/03/2024
Es día cero (0 day):	No

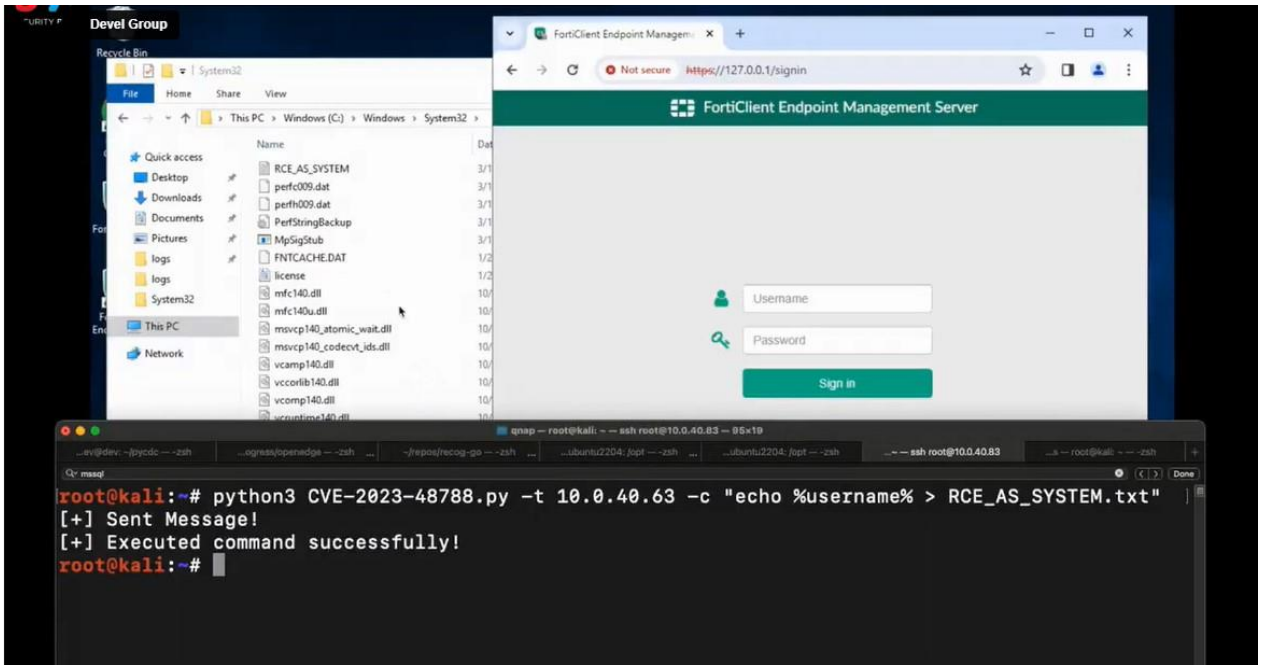
RESUMEN

El mundo en constante evolución de la ciberseguridad, cada nueva vulnerabilidad descubierta representa un desafío significativo para las empresas que dependen de tecnologías de red confiables. Recientemente, Fortinet, un importante proveedor de soluciones de seguridad informática, ha emitido una advertencia sobre una vulnerabilidad crítica de ejecución remota de código (RCE) en su servidor de gestión empresarial FortiClient EMS. Esta vulnerabilidad, identificada como CVE-2024-48788, plantea una amenaza considerable para la seguridad de los sistemas informáticos, permitiendo a los atacantes ejecutar código arbitrario con privilegios de administrador en sistemas afectados.

La vulnerabilidad CVE-2024-48788 se origina en un error de inyección SQL en un componente de almacenamiento directamente adjunto al servidor. Esto proporciona a los atacantes no autenticados la capacidad de ejecutar código y comandos maliciosos en sistemas vulnerables mediante solicitudes especialmente diseñadas. La gravedad de esta vulnerabilidad ha sido clasificada como crítica, con una puntuación de 9.3 sobre 10 en la escala CVSS, lo que subraya la urgencia de abordar este problema de seguridad.

Esta vulnerabilidad afecta a las siguientes versiones:

- FortiClientEMS 7.2.0 a través de 7.2.2 (Actualizar a 7.2.3 o superior)
- FortiClientEMS 7.0.1 a través de 7.0.10 (Actualizar a 7.0.11 o superior)



Según el aviso de Fortinet, la vulnerabilidad podría ser explotada por atacantes no autenticados para ejecutar código o comandos no autorizados a través de solicitudes específicamente diseñadas. La

explotación exitosa de esta falla podría llevar a la ejecución remota de código en el servidor, lo que potencialmente comprometería la seguridad y la integridad de los sistemas.

El investigador Thiago Santana del equipo de desarrollo de FortiClientEMS y el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC) fueron acreditados por descubrir y reportar la falla.

Si bien actualmente no hay evidencia de explotación activa de esta vulnerabilidad, es fundamental que las organizaciones afectadas apliquen los parches de seguridad proporcionados por Fortinet lo antes posible para mitigar los riesgos asociados con esta vulnerabilidad.

En otro informe relacionado, el equipo de investigación de Horizon3.ai reveló detalles adicionales sobre 16 fallas que reportaron a Fortinet en 2023. Aunque la mayoría de estas fallas han sido parcheadas por la compañía, dos de ellas relacionadas con las tecnologías FortiWLM y FortiSIEM aún no han sido solucionadas.

Estas vulnerabilidades no resueltas podrían permitir a los atacantes realizar acciones maliciosas, como la obtención de archivos de registro arbitrarios o la toma de sesiones de administrador. Por lo tanto, se recomienda a las organizaciones afectadas que estén atentas a futuras actualizaciones de seguridad y que apliquen los parches disponibles tan pronto como sea posible para proteger sus sistemas contra posibles ataques.

La persistencia de vulnerabilidades críticas en el software de Fortinet subraya la importancia de una gestión proactiva de la seguridad cibernética en el entorno empresarial actual. Al mantenerse al tanto de las últimas amenazas de seguridad y tomar medidas preventivas adecuadas, las organizaciones pueden fortalecer su postura de seguridad y proteger sus activos digitales de posibles ataques cibernéticos.

NOTICIA COMPLETA

https://devel.group/blog/fortinet-alerta-sobre-una-nueva-vulnerabilidad-critica-de-ejecucion-remota-de-codigo/

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