Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA EN FORTISIEM (CVE-2025-25256) CON EXPLOTACIÓN ACTIVA

13/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

En un contexto donde las amenazas cibernéticas evolucionan con rapidez y los atacantes buscan vulnerar los sistemas más críticos, las herramientas de gestión y monitoreo de seguridad se han convertido en objetivos estratégicos. Fortinet ha emitido una alerta urgente sobre una vulnerabilidad crítica en su solución FortiSIEM, catalogada como CVE-2025-25256, que ya cuenta con código de explotación circulando activamente en la red. La severidad de este fallo, con una puntuación CVSS de 9.8 sobre 10, subraya el potencial impacto que podría tener en organizaciones que no actúen de inmediato.

La falla, de tipo inyección de comandos en el sistema operativo, permite a un atacante no autenticado ejecutar instrucciones arbitrarias en el entorno afectado. Esta situación, agravada por la ausencia de indicadores de compromiso visibles, dificulta la detección temprana y aumenta la probabilidad de intrusiones exitosas. Ante este escenario, las empresas deben priorizar la actualización a versiones seguras y aplicar medidas de mitigación para reducir el riesgo operativo y de seguridad.

GUNRA RANSOMWARE: NUEVA VARIANTE PARA LINUX REFUERZA CAPACIDADES DE CIFRADO MASIVO Y PERSONALIZACIÓN

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

ID de alerta:	DSOC-CERT_2025_13_02_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/08/2025
Es día cero (0 day):	No

RESUMEN

Fortinet ha emitido una advertencia urgente sobre una vulnerabilidad crítica en FortiSIEM, identificada como CVE-2025-25256, que ya cuenta con código de explotación activo en entornos reales. El fallo posee una puntuación CVSS de 9.8/10, lo que indica un riesgo extremadamente alto para las organizaciones que utilicen versiones afectadas.

Descripción técnica de la vulnerabilidad

El problema radica en una inyección de comandos del sistema operativo (OS Command Injection – CWE-78).

Esto permite que un atacante no autenticado ejecute comandos o código malicioso en el sistema mediante peticiones CLI manipuladas, comprometiendo por completo la integridad del entorno.

Versiones afectadas y acciones recomendadas

Las versiones vulnerables de **FortiSIEM** son:

- **6.1, 6.2, 6.3, 6.4, 6.5, 6.6** → Migrar a una versión corregida.
- **6.7.0 a 6.7.9** → Actualizar a **6.7.10 o superior**.
- **7.0.0 a 7.0.3** → Actualizar a **7.0.4 o superior**.
- **7.1.0 a 7.1.7** → Actualizar a **7.1.8 o superior**.
- **7.2.0 a 7.2.5** → Actualizar a **7.2.6 o superior**.
- **7.3.0 a 7.3.1** → Actualizar a **7.3.2 o superior**.

Riesgo e impacto empresarial

Fortinet ha confirmado que ya se ha detectado código de explotación funcional circulando en la red, aunque no ha dado detalles de su origen ni de campañas específicas.
Un punto crítico: no existen indicadores de compromiso (IoCs) fácilmente detectables, lo que dificulta la identificación de incidentes.

Medidas de mitigación urgentes

Mientras se aplican las actualizaciones, se recomienda:

1. Limitar el acceso al puerto phMonitor (7900) exclusivamente a direcciones IP autorizadas.
2. Monitorear actividades anómalas en FortiSIEM, aunque la ausencia de IoCs obliga a reforzar la supervisión general del sistema.
3. Aislar entornos críticos de exposición directa a Internet.

Contexto adicional de amenazas

Esta advertencia surge un día después de que investigadores reportara un aumento significativo en ataques de fuerza bruta contra Fortinet SSL VPN, con origen en múltiples países, incluyendo Estados Unidos, Canadá, Rusia y Países Bajos.
Esto refuerza la necesidad de mantener una política de actualizaciones proactiva y aplicar segmentación de red.

Recomendación final: Las organizaciones que utilicen FortiSIEM deben actuar de inmediato para aplicar los parches o migrar a versiones seguras. La explotación activa y la ausencia de IoCs hacen que la ventana de respuesta sea extremadamente reducida.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-en-fortisiem-cve-2025-25256-con-explotacion-activa/

CONTACTOS DE SOPORTE

Correo electrónico: cti@devel.group

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://devel.group/