Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET CORRIGE VULNERABILIDAD CRÍTICA ZERO-DAY EN SUS PRODUCTOS

14/ 05 / 2025

CONTENIDO

INTRODUCCIÓN

Fortinet, una de las empresas líderes en soluciones de ciberseguridad empresarial, ha emitido una alerta crítica sobre una vulnerabilidad grave que afecta a varios de sus productos, incluyendo sistemas de telefonía, correo electrónico y grabación de video. La falla, identificada como CVE-2025-32756, ya está siendo explotada por atacantes en el mundo real, lo que la convierte en una amenaza inmediata para organizaciones que aún no han aplicado las correcciones necesarias.

El problema permite que un atacante sin autenticación previa tome control remoto de los sistemas vulnerables simplemente enviando solicitudes maliciosas a través de Internet. Esto representa un riesgo elevado de robo de información, interrupción de servicios y compromiso total del sistema afectado. En esta nota explicamos en lenguaje simple qué ocurrió, qué productos están en riesgo, y qué medidas tomar para protegerse.

FORTINET CORRIGE VULNERABILIDAD CRÍTICA ZERO-DAY EN SUS PRODUCTOS

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

ID de alerta:	DSOC-CERT_2025_05_14_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/05/2025
Es día cero (0 day):	Sí

RESUMEN

¿Qué está pasando?
La reconocida empresa de ciberseguridad Fortinet ha solucionado una grave vulnerabilidad de seguridad que estaba siendo aprovechada activamente por atacantes. Esta falla, identificada como CVE-2025-32756, afecta a varios de sus productos más utilizados en entornos corporativos, incluyendo FortiVoice, un sistema de telefonía empresarial.

En palabras simples, ¿qué significa esto?
Un fallo de programación en el manejo de datos (lo que se conoce como un desbordamiento de pila, o *stack overflow*) permitía a criminales informáticos tomar el control total de un sistema vulnerable sin necesidad de tener una cuenta o acceso previo. Bastaba con enviar una solicitud maliciosa a través de Internet para explotar el fallo.

Nivel de gravedad

Métrica	Detalle
CVE	CVE-2025-32756
Puntuación CVSS	9.6 / 10 (Crítica)
Tipo de fallo	Ejecución remota de código (*Remote Code Execution – RCE*)
Productos afectados	FortiVoice, FortiMail, FortiNDR, FortiRecorder, FortiCamera

¿Ya lo estaban explotando?
Sí. Fortinet confirmó que los atacantes ya estaban usando esta vulnerabilidad, específicamente en sistemas FortiVoice, antes de que se publicara la solución.

¿Qué hicieron los atacantes?
Los cibercriminales fueron más allá de solo explotar la falla:

- Escanearon redes completas en busca de otros dispositivos.
- Borraron los registros del sistema para ocultar su rastro.
- Activaron funciones especiales para robar credenciales (usuarios y contraseñas).

Además, Fortinet identificó las direcciones IP desde donde se originaron estos ataques:

- 198[.]105[.]127[.]124
- 43[.]228[.]217[.]173
- 43[.]228[.]217[.]82
- 156[.]236[.]76[.]90
- 218[.]187[.]69[.]244
- 218[.]187[.]69[.]59

¿Qué hacer si uso productos Fortinet?

Si su empresa y/u organización utiliza alguno de los siguientes productos, es urgente que actualice a las versiones corregidas:

Versión	Afectadas	Solución
FortiCamera 2.1	2.1.0 hasta 2.1.3	Actualizar a 2.1.4 o superior
FortiCamera 2.0	Todas las versiones 2.0	Migrar a una versión corregida
FortiCamera 1.1	Todas las versiones 1.1	Migrar a una versión corregida
FortiMail 7.6	7.6.0 hasta 7.6.2	Actualizar a 7.6.3 o superior
FortiMail 7.4	7.4.0 hasta 7.4.4	Actualizar a 7.4.5 o superior
FortiMail 7.2	7.2.0 hasta 7.2.7	Actualizar a 7.2.8 o superior
FortiMail 7.0	7.0.0 hasta 7.0.8	Actualizar a 7.0.9 o superior
FortiNDR 7.6	7.6.0	Actualizar a 7.6.1 o superior
FortiNDR 7.4	7.4.0 hasta 7.4.7	Actualizar a 7.4.8 o superior
FortiNDR 7.2	7.2.0 hasta 7.2.4	Actualizar a 7.2.5 o superior
FortiNDR 7.1	Todas las versiones 7.1	Migrar a una versión corregida
FortiNDR 7.0	7.0.0 hasta 7.0.6	Actualizar a 7.0.7 o superior
FortiNDR 1.5	Todas las versiones 1.5	Migrar a una versión corregida
FortiNDR 1.4	Todas las versiones 1.4	Migrar a una versión corregida
FortiNDR 1.3	Todas las versiones 1.3	Migrar a una versión corregida
FortiNDR 1.2	Todas las versiones 1.2	Migrar a una versión corregida
FortiNDR 1.1	Todas las versiones 1.1	Migrar a una versión corregida
FortiRecorder 7.2	7.2.0 hasta 7.2.3	Actualizar a 7.2.4 o superior
FortiRecorder 7.0	7.0.0 hasta 7.0.5	Actualizar a 7.0.6 o superior
FortiRecorder 6.4	6.4.0 hasta 6.4.5	Actualizar a 6.4.6 o superior
FortiVoice 7.2	7.2.0	Actualizar a 7.2.1 o superior
FortiVoice 7.0	7.0.0 hasta 7.0.6	Actualizar a 7.0.7 o superior
FortiVoice 6.4	6.4.0 hasta 6.4.10	Actualizar a 6.4.11 o superior

Consulte las versiones específicas y actualice según las recomendaciones oficiales. Si no puede actualizar de inmediato, desactiva el acceso HTTP/HTTPS a la interfaz de administración como medida temporal.

Conclusión para principiantes
En ciberseguridad, una “vulnerabilidad” es como una puerta secreta que los atacantes pueden usar para entrar a tu casa digital. En este caso, esa puerta estaba abierta y siendo utilizada activamente. Si usa productos Fortinet, actualizar es la única forma de cerrarla completamente.

NOTICIA COMPLETA

https://devel.group/blog/fortinet-corrige-vulnerabilidad-critica-zero-day-en-sus-productos/

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://devel.group/