Nro. Alerta:	AL-2025-018	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	15-may-2025	**FORTINET**(CVE-2025-32756)	Pág.: **1** of **1**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Información
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- FORTINET - figura referencial

Fortinet ha revelado una vulnerabilidad crítica de desbordamiento de búfer basada en pila [CWE-121], identificada como CVE-2025-32756 afecta a una amplia gama de sus productos de seguridad y red.

III. INTRODUCCIÓN

Esta vulnerabilidad de desbordamiento basada en pila afecta a los productos FortiVoice, FortiMail, FortiNDR, FortiRecorder y FortiCamera lo cual podría permitir que un atacante remoto no autenticado ejecute código o comandos arbitrarios mediante solicitudes HTTP.

Fortinet ha observado la explotación en el campo sobre todo en el producto FortiVoice.

IV. VECTOR DE ATAQUE

El ataque se produce mediante el envío de **solicitudes HTTP manipuladas** a los dispositivos vulnerables, explotando el desbordamiento de búfer para ejecutar código arbitrario

sin autenticación previa. En incidentes confirmados, los atacantes realizaron las siguientes acciones:

- Escaneo de redes internas.
- Habilitación maliciosa del modo de depuración FCGI para extraer credenciales.
- Eliminación de registros de fallos (crashlogs) para ocultar rastros.
- Creación de archivos y procesos maliciosos.
- Inclusión de trabajos `cron` para exfiltrar información.

V. IMPACTO

Afectación de productos por vulnerabilidades:

(CVE-2025-32756)

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

Tabla 1.-Versiones Afectadas - FORTINET

- Ejecución remota de código en los dispositivos afectados.
- Potencial compromiso completo del sistema.

- Intercepción de comunicaciones sensibles.
- Eliminación de registros para evitar la detección.
- Instalación de puertas traseras y malware persistente.
- Expansión lateral dentro de la red interna.

VI. INDICADORES DE COMPROMISO

Direcciones IP usadas por Actor de amenazas
198.105.127{.}124
43.228.217{.}173
43.228.217{.}82
156.236.76{.}90
218.187.69{.}244
218.187.69{.}59

Tabla 2.- (IoC) vinculados- FORTINET

Archivos
4410352e110f82eabc0bf160bec41d21
ebce43017d2cb316ea45e08374de7315
489821c38f429a21e1ea821f8460e590
364929c45703a84347064e2d5de45bcd
2c8834a52faee8d87cff7cd09c4fb946

Tabla 3.- (IoC) vinculados- FORTINET

VII. RECOMENDACIONES:

Fortinet recomienda aplicar parches de inmediato y en caso de no poder a hacerlo sugiere:

- Deshabilitar las interfaces administrativas HTTP/HTTPS
- Restringir el acceso administrativo a redes internas de confianza
- Monitorear los dispositivos afectados para detectar IoC conocidos

Verificar si la depuración FCGI ha sido habilitada maliciosamente mediante el comando:

```
nginx

diag debug application fcgi
```

Si el resultado incluye: general to-file ENABLED, esto es un fuerte **indicador de compromiso**.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://fortiguard.fortinet.com/psirt/FG-IR-25-254

https://csirt.axtel.com.mx/bulletin/post/314

https://blog.segu-info.com.ar/2025/05/falla-critica-en-fortinet-explotado.html?m=1

https://es.linkedin.com/pulse/falla-cr%C3%ADtica-en-fortinet-explotado-activamente-cve-2025-32756-cbkac