Boletín de alerta

Boletín Nro.: 47
Fecha de publicación: 26/05/2025
Tema: Alerta 2025-47 Vulnerabilidad crítica Zero-Day en FortiClientEMS
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- **FortiCamera:**
  - Versiones 2.1.0 a 2.1.3
  - Todas las versiones 2.0
  - Todas las versiones 1.1
- **FortiMail:**
  - Versiones 7.6.0 a 7.6.2
  - Versiones 7.4.0 a 7.4.4
  - Versiones 7.2.0 a 7.2.7
  - Versiones 7.0.0 a 7.0.8
- **FortiNDR:**
  - Versión 7.6.0
  - Versiones 7.4.0 a 7.4.7
  - Versiones 7.2.0 a 7.2.4
  - Todas las versiones 7.1
  - Versiones 7.0.0 a 7.0.6
  - Todas las versiones 1.5, 1.4, 1.3, 1.2, 1.1
- **FortiRecorder:**
  - Versiones 7.2.0 a 7.2.3
  - Versiones 7.0.0 a 7.0.5
  - Versiones 6.4.0 a 6.4.5
- **FortiVoice**:
  - Versión 7.2.0
  - Versiones 7.0.0 a 7.0.6
  - Versiones 6.4.0 a 6.4.10

Descripción

El equipo de Fortinet Product Security identificó una **vulnerabilidad crítica activamente explotada**, identificada como **CVE-2025-32756**, de desbordamiento de bufer basado en pila (stack-based buffer overflow) que afecta varios productos Fortinet, incluyendo FortiVoice, FortiMail, FortiNDR, FortiRecorder y FortiCamera. Esta vulnerabilidad se origina por una falla en la validación de límites durante el procesamiento de peticiones HTTP, lo que permite a un atacante remoto no autenticado enviar solicitudes HTTP especialmente diseñadas para provocar un desbordamiento de pila.

La explotación exitosa **permite a un atacante ejecutar código arbitrario o comandos con privilegios elevados** en el dispositivo afectado, lo que puede derivar en un compromiso total del sistema. En particular, en FortiVoice se ha confirmado explotación activa en entornos reales, donde los atacantes han logrado:

- Examinar la red del dispositivo
- Borrar registros de fallos del sistema
- Registrar credenciales del sistema

La gravedad de **esta vulnerabilidad es crítica**, con una puntuación **CVSS de 9.8**, reflejando su alto impacto y facilidad de explotación remota sin necesidad de autenticación previa

Solución:

Recomendaciones y Medidas de Mitigación:

Fortinet ha publicado actualizaciones para mitigar esta vulnerabilidad en los productos afectados. Se recomienda encarecidamente actualizar a las siguientes versiones o superiores:

- **FortiVoice:**
  - 7.2.x: actualizar a 7.2.1 o superior
  - 7.0.x: actualizar a 7.0.7 o superior
  - 6.4.x: actualizar a 6.4.11 o superior
- **FortiCamera:** Actualizar a la última versión disponible que corrige la vulnerabilidad (consultar aviso oficial Fortinet).
- **FortiMail, FortiNDR, FortiRecorder:** Actualizar a las versiones parcheadas indicadas en los avisos oficiales de Fortinet.

Además, se recomienda:

- Monitorizar la activación maliciosa de la depuración FCGI con el comando:
  diag debug application fcgi
  Si el resultado muestra general to-file ENABLED, es un indicador fuerte de explotación activa.
- Implementar medidas de mitigación temporales si no es posible actualizar inmediatamente, como restringir el acceso a interfaces de administración y monitorear tráfico HTTP sospechoso.

Para más información visita la página de Fortinet donde se pueden descargar los últimos parches de seguridad: https://fortiguard.fortinet.com/psirt/FG-IR-25-254

Información adicional:

Security Advisory: CVE-2025-32756 – Critical Stack-Based Buffer Overflow in Fortinet Products

NVD – CVE-2025-32756

Falla crítica en Fortinet explotado activamente (CVE-2025-32756).

PSIRT | FortiGuard Labs