LUMA

BOLETÍN DE SEGURIDAD CIBERNÉTICA

14 de Mayo 2025

TLP: CLEAR

Vulnerabilidad CVE-2025-22252 Omisión de autenticación TACACS+

Impacto:
Critico - 9.0

Publicado: 2025-05-13
Actualizado: 2025-05-13

Descripción:

Una vulnerabilidad relacionada con la falta de autenticación en funciones críticas (CWE-306) afecta a FortiOS, FortiProxy y FortiSwitchManager cuando están configurados para utilizar TACACS+ con un servidor remoto que emplea autenticación ASCII. Esta falla podría permitir que un atacante que conozca las credenciales de una cuenta administrativa obtenga acceso al dispositivo con privilegios de administrador, saltándose el proceso de autenticación.

Recursos Afectados:

Esta vulnerabilidad limita a configuraciones donde se utiliza autenticación ASCII.

Solución:

Para remediar CVE-2025-22252, aplicar parches de seguridad según el producto y versión afectada, mostradas en la siguiente tabla:

Producto	Versión Afectada	Versión Fija / Solución
FortiOS 7.6	7.6.0	Actualizar a **7.6.1** o superior
FortiOS 7.4	7.4.4 a 7.4.6	Actualizar a **7.4.7** o superior
FortiProxy 7.6	7.6.0 a 7.6.1	Actualizar a **7.6.2** o superior
FortiSwitchManager 7.2	7.2.5	Actualizar a **7.2.6** o superior

Referencias:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-472
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-fortinet-2

Vulnerabilidad CVE-2025-47295 Sobre lectura de búfer en FGFM

Impacto:
Bajo – 3.4

Publicado: 2025-05-13

Descripción:

Una vulnerabilidad de tipo buffer over-read ([CWE-126]) detectada en FortiOS podría ser explotada por un atacante remoto no autenticado para provocar la interrupción del servicio del demonio FGFM. Esta explotación sería posible mediante el envío de una solicitud específicamente manipulada, aunque solo bajo condiciones poco frecuentes que escapan al control del atacante.

Solución:

Para remediar CVE-2025-47295, aplicar parches de seguridad según el producto y versión afectada, mostradas en la siguiente tabla:

Versión	Afectado	Solución
FortiOS 7.4	7.4.0 a 7.4.3	Actualice a 7.4.4 o superior
FortiOS 7.2	7.2.0 a 7.2.7	Actualice a 7.2.8 o superior
FortiOS 7.0	7.0.0 a 7.0.14	Actualice a 7.0.15 o superior
FortiOS 6.4	6.4 todas las versiones	Migrar a una versión fija

Referencias:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-381

Denegación de servicio en la raíz de Security Fabric

Impacto:
Medio – 4.8

CVE:
CVE-2025-47294
Publicado: 2025-05-13

Descripción:

Una vulnerabilidad de tipo integer overflow o desbordamiento de enteros ([CWE-190]) identificada en el componente Security Fabric de FortiOS podría ser aprovechada por un atacante remoto no autenticado para provocar una interrupción del servicio del demonio csfd, mediante el envío de una solicitud específicamente construida con fines maliciosos.

Recursos Afectados:

Security Fabric Root de FortiOS.

Solución:

Para remediar CVE-2025-47294, aplicar parches de seguridad según el producto y versión afectada, mostradas en la siguiente tabla:

Versión	Afectado	Solución
FortiOS 7.2	7.2.0 a 7.2.7	Actualice a 7.2.8 o superior
FortiOS 7.0	7.0.0 a 7.0.14	Actualice a 7.0.15 o superior
FortiOS 6.4	6.4 todas las versiones	Migrar a una versión fija

Referencias:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-388

Desbordamiento de búfer basada en pila en la API

Impacto:
Critico – 9.6

CVE:
CVE-2025-32756
Publicado: 2025-05-13

Descripción:

Fortinet ha informado sobre una vulnerabilidad crítica de desbordamiento de búfer en pila (stack-based buffer overflow, CWE-121), identificada como CVE-2025-32756. Esta falla afecta a varios productos de la compañía, entre ellos FortiVoice, FortiMail, FortiNDR, FortiRecorder y FortiCamera. Está siendo explotada activamente, principalmente en dispositivos FortiVoice.

Las operaciones realizadas por el Actor de Amenaza en el caso que observamos fueron parte o todas las siguientes:

- Escanear la red del dispositivo
- Borrar registros de fallos del sistema
- Habilite la depuración de fcgi para registrar las credenciales del sistema o los intentos de inicio de sesión SSH

Solución:

Deshabilitar la interfaz administrativa HTTP/HTTPS, es decir, deshabilitar servicios HTTP/HTTPS en interfaces administrativas externas hasta que se apliquen las actualizaciones respectivas.

Para remediar CVE-2025-47294, aplicar parches de seguridad según el producto y versió la siguiente tabla:

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

IoC´s

Direcciones IP:

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

Referencias:

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