TLP: CLEAR

BOLETÍN DE CIBERSEGURIDAD

16 de Mayo 2025

Vulnerabilidad CVE-2025-22252 Omisión de autenticación TACACS+

Impacto:
Critico - 9.0

Descripcion:
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

Fuentes de información:
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

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

Fuentes de informacion:

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

Denegación de servicio en la raíz de Security Fabric

Impacto:
Medio – 4.8

Descripción:

Una vulnerabilidad de tipo integer overflow o desbordamiento de enteros ([CWE-190])identificada en el componente Security Fabric de FortiOS podría ser aprovechada porun 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

Fuentes de información:

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

Desbordamiento de búfer basada en pila en la API

Impacto:

Medio – 4.8

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

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

versión afectada, mostradas en 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

Fuentes de informacion:

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

VMware Tools Vulnerability Let

Impacto:
Medio – 6.1

Una vulnerabilidad de gravedad moderada en VMware Tools podría permitir a atacantes con privilegios limitados manipular archivos y activar operaciones inseguras dentro de máquinas virtuales. La vulnerabilidad, identificada como CVE-2025-22247, afecta a las versiones para Windows y Linux de VMware Tools 11.xx y 12.xx. Se ha confirmado que las versiones para macOS no se ven afectadas.

Dado que actualmente no existen soluciones alternativas y la explotación podría comprometer la integridad de las máquinas virtuales afectadas, se recomienda encarecidamente aplicar los parches correspondientes lo antes posible.

Según el aviso de Broadcom, la vulnerabilidad en el manejo inseguro de archivos permite que un actor malicioso con privilegios no administrativos en una máquina virtual invitada manipule archivos locales para activar operaciones inseguras dentro de esa máquina virtual. Esta falla ha recibido una puntuación base CVSSv3 de 6.1, lo que la clasifica como de gravedad moderada.

El investigador de seguridad Sergey Bliznyuk, de Positive Technologies, fue quien descubrió y notificó la vulnerabilidad a VMware.

Este nuevo problema de seguridad se presenta tras la divulgación de varias otras vulnerabilidades en productos VMware a comienzos de este año, entre ellas una vulnerabilidad crítica de tipo TOCTOU (Time-of-Check to Time-of-Use), identificada como **CVE-2025-22224**, que afecta a VMware ESXi y Workstation. Esta falla podría permitir escrituras fuera de límites y la posible ejecución de código.

Este tipo de vulnerabilidad resulta especialmente preocupante en entornos virtualizados donde múltiples inquilinos comparten una misma infraestructura física. Aunque el impacto directo se limita a la máquina virtual invitada, la falla podría ser aprovechada como parte de una cadena de ataque más compleja o para lograr la escalada de privilegios dentro de la misma máquina virtual.

Factores de riesgo	Detalles
Productos afectados	Herramientas de VMware 11.xx, 12.xx (Windows/Linux)
Impacto	Manipulación de archivos que permite operaciones maliciosas en máquinas virtuales invitadas
Requisitos previos de explotación	Privilegios no administrativos en una máquina virtual invitada
Puntuación CVSS 3.1	6.1 (Moderado)

Mitigaciones:

Broadcom ha lanzado la versión **12.5.2 de VMware Tools** para corregir la vulnerabilidad **CVE-2025-22247** en sistemas Windows y Linux. En el caso específico de sistemas Windows de 32 bits, la versión **12.4.7 de VMware Tools**, incluida dentro del paquete 12.5.2, resuelve el problema.

Para los sistemas Linux, se informa que la versión corregida de **open-vmtools** será distribuida por los respectivos proveedores de cada distribución. Es importante tener en cuenta que las versiones específicas pueden variar dependiendo del proveedor y la distribución utilizada.

Esta vulnerabilidad afecta al software VMware ampliamente desplegado en entornos de virtualización empresarial, por lo que se recomienda aplicar las actualizaciones correspondientes a la mayor brevedad posible.

Fuentes de información:
https://cybersecuritynews.com/vmware-toolsvulnerability/

Actualización de Seguridad de SAP

Impacto:
Critica – 7.1

Descripción:

SAP ha publicado su boletín mensual en el que se incluyen 16 vulnerabilidades: 1 de severidad crítica, 4 altas y 11 medias. Estas vulnerabilidades afectan a varios de sus productos y su explotación podría permitir a un atacante comprometer la confidencialidad, integridad y disponibilidad del sistema host.

Detalle:

La vulnerabilidad de severidad crítica afecta al cargador de metadatos de SAP NetWeaver Visual Composer que es vulnerable cuando un usuario con privilegios de administrador puede cargar contenido malicioso o no confiable que, al deserializarse, podría comprometer la confidencialidad, integridad y disponibilidad del sistema host. Se ha asignado el identificador CVE-2025-42999 para esta vulnerabilidad.

Recursos Afectados

- SAP NetWeaver;
- AP Supplier Relationship Management;
- SAP S/4HANA Cloud Private Edition u On Premise;
- SAP Business Objects Business Intelligence Platform (PMW);

- SAP Landscape Transformation;
- SAP PDCE;
- SAP Gateway Client;
- SAP S/4HANA;
- SAP Service Parts Management (SPM);
- SAP NetWeaver Application Server ABAP y ABAP Platform;
- SAP Supplier Relationship Management;
- SAP S/4HANA HCM Portugal y SAP ERP HCM Portugal;
- SAP Digital Manufacturing;
- SAP Data Services Management Console;
- SAP GUI para Windows.

Solución:

El fabricante recomienda encarecidamente que el cliente visite el portal de soporte y aplique los parches de forma prioritaria para proteger su entorno SAP.

Para ver el detalle del resto de vulnerabilidades se recomienda visitar el aviso oficial enlazado en la sección de referencias.

Fuentes de información:

SAP Security Patch Day – May 2025

SAP Security Notes: May 2025 Patch Day - Onapsis

Actualización de Seguridad de Windows

Impacto:
Critica – 7.1

Microsoft ha corregido 72 vulnerabilidades en su lanzamiento de actualizaciones de seguridad de mayo de 2025. Los parches de este mes incluyen correcciones para cinco vulnerabilidades de «zero-day» explotadas activamente.

Microsoft parcheó un total de cinco vulnerabilidades críticas y 62 vulnerabilidades adicionales de distintos niveles de gravedad.

Vulnerabilidades de Zero-Day explotadas activamente en el sistema de archivos de registro común de Windows

CVE-2025-32706 es una importante vulnerabilidad de elevación de privilegios que afecta al sistema de archivos de registro común de Windows y tiene una puntuación CVSS de 7,8. Este defecto permite a un atacante local autenticado ejecutar código con privilegios elevados del sistema debido a una validación de entrada incorrecta.

Esta vulnerabilidad de «zero-day» fue descubierta a finales de abril de 2025 por CrowdStrike Counter Adversary Operations, que reveló responsablemente la vulnerabilidad a Microsoft a través de canales privados. Posteriormente, Microsoft validó el problema y publicó un parche para solucionarlo el (13 de mayo de 2025).

CVE-2025-32701 es una importante vulnerabilidad de elevación de privilegios que afecta al sistema de archivos de registro común de Windows y tiene una puntuación CVSS de 7,8. Se trata de una vulnerabilidad de uso después de la liberación que, si se explota con éxito, podría permitir a un atacante elevar privilegios en el sistema afectado.

CVE-2025-30400 es una importante vulnerabilidad de elevación de privilegios que afecta a la biblioteca central de Microsoft Desktop Windows Manager (DWM) y tiene una puntuación CVSS de 7,8. Un atacante puede explotar esta vulnerabilidad convenciendo a un usuario para que abra un archivo o sitio web especialmente diseñado, lo que le permite ejecutar código arbitrario con los privilegios del usuario. Aunque no se ha publicado una prueba de concepto pública, Microsoft ha confirmado que esta vulnerabilidad está siendo explotada en la actualidad.

CVE-2025-30397 es una importante vulnerabilidad de corrupción de memoria que afecta al motor de scripting de Microsoft y tiene una puntuación CVSS de 7,5. Esto podría permitir a un atacante remoto ejecutar código si un usuario hace clic en un enlace malicioso mientras utiliza el modo Internet Explorer de Microsoft Edge. El ataque requiere la interacción del usuario y tiene una alta complejidad de ataque. Aunque no se ha revelado la prueba de concepto de esta vulnerabilidad, Microsoft ha confirmado que se ha explotado activamente en la naturaleza.

CVE-2025-29966 y **CVE-2025-29967** son vulnerabilidades críticas de ejecución remota de código (RCE) que afectan a los Servicios de Escritorio Remoto de Microsoft Windows, y ambas tienen una puntuación CVSS de 8,8. Se ha descubierto una vulnerabilidad de desbordamiento de búfer basada en heap en Windows Remote Desktop. Podría permitir a atacantes remotos con control de un Servidor de Escritorio Remoto desencadenar la ejecución remota de código en una máquina Cliente RDP que se conecte al servidor malicioso. Se trata de una

vulnerabilidad del lado del cliente que no requiere autenticación ni interacción, lo que podría llevar a la toma completa del sistema.

CVE-2025-30377 y **CVE-2025-30386** son vulnerabilidades RCE críticas que afectan a Microsoft Office, y ambas tienen una puntuación CVSS de 8,4. Se trata de vulnerabilidades «use-after-free» que requieren que un atacante convenza a una víctima para que abra un archivo especialmente diseñado, con el panel de vista previa como vector de ataque adicional. Preview Pane se ha visto muchas veces en otras vulnerabilidades (abril de 2023, julio de 2023, diciembre de 2023, octubre de 2024, enero de 2025, febrero de 2025, abril de 2025).

CVE-2025-29833 es una vulnerabilidad RCE crítica que afecta a Windows Virtual Machine Bus y tiene una puntuación CVSS de 7,1. Existe una vulnerabilidad de race condition de tiempo de comprobación de tiempo de uso (TOCTOU) en Windows Virtual Machine Bus que permite a los atacantes ejecutar código arbitrario a través de una red. TOCTOU es un tipo específico de vulnerabilidad de condición de carrera que se produce cuando hay un intervalo de tiempo entre la comprobación del estado de un recurso y el uso de ese recurso.

Para ver el detalle del resto de vulnerabilidades de Windows se recomienda visitar el sitio oficial.

https://msrc.microsoft.com/update-guide/releaseNote/2025-May

Fuentes de información:

Actualizaciones de seguridad de Microsoft de mayo de 2025 | INCIBE-CERT | INCIBE