PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

124-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°124	Fecha: 28-05-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	BadSuccessor: escalamiento de privilegios abusando de dMSA en Active Directory		
Tipo de Ataque	Intento de acceso con vulneración de credenciales	Abreviatura	IAVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Investigadores de Akamai descubren un fallo crítico en el uso de cuentas de servicio delegadas (dMSA) que expone a organizaciones con Windows Server 2025 a ataques de escalada de privilegios.

2. **DETALLES:**

Esta técnica avanzada de escalamiento de privilegios en entornos Windows Server 2025 conocida como BadSuccessor depende de una nueva funcionalidad legítima: las Cuentas de Servicio Administradas delegadas (dMSA), las cuales fueron introducidas en Windows Server 2025 como una mejora sobre las Managed Service Accounts (MSA) y Group Managed Service Accounts (gMSA).

Su objetivo es permitir una gestión centralizada, segura y delegada de cuentas de servicio, incluyendo:

- Rotación automática de contraseñas.
- Restricción por máquina (sólo equipos autorizados pueden usarla).
- Delegación de control para facilitar la administración sin comprometer el principio de privilegios mínimos.

Sin embargo, el mecanismo de migración de estas cuentas puede ser manipulado para heredar permisos de cualquier cuenta, incluidos administradores de dominio, sin requerir privilegios elevados.

BadSuccessor permite a cualquier usuario que tenga permisos para crear objetos dMSA —algo común en ciertos entornos con delegación mal configurada— vincular una nueva dMSA con cualquier otra cuenta del dominio (incluidos Domain Admins), simplemente modificando dos atributos:

- msDS-ManagedAccountPrecededByLink: que establece la cuenta “heredada”.
- msDS-DelegatedMSAState: que simula una migración completada.

Una vez establecido el vínculo, el Centro de Distribución de Claves, al generar el ticket de autenticación para la dMSA, añade los privilegios y grupos de la cuenta original al nuevo objeto, sin ningún tipo de validación adicional.

Microsoft ha reconocido el problema, pero aún no ha publicado un parche.

3. **RECOMENDACIONES:**

- Auditar la creación de dMSAs mediante el evento ID 5137, y monitorizar cambios en el atributo msDS-ManagedAccountPrecededByLink con el evento ID 5136.
- Revisar autenticaciones dMSA mediante eventos ID 2946, que revelan cuándo un TGT se genera con el paquete de claves heredado.
- Restringir quién puede crear dMSAs, especialmente en contenedores y Unidades Organizativas (OUs).
- Utilizar herramientas de auditoría para identificar todos los usuarios con permisos CreateChild.
- Aplicar el principio de mínimo privilegio a la gestión de cuentas de servicio.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/05/badsuccessor-escalamiento-de.html • hxxps://revistacloud.com/badsuccessor-una-nueva-vulnerabilidad-en-windows-server-2025-permite-comprometer-dominios-de-active-directory/ • hxxps://www.hackplayers.com/2025/05/badsuccessor-escalada-de-privilegios.htm

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°124	Fecha: 28-05-2025 Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Evertz SDVN 3080ipx-10G		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comandos que afecta a la línea de productos de Red de Vídeo Definida por Software (SDVN) de Evertz, incluyendo el 3080ipx-10G y otros dispositivos ampliamente utilizados en infraestructuras de radiodifusión. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios del sistema como root sin autenticación, lo que supone un grave riesgo de comprometer completamente.

2. DETALLES:

Evertz SDVN 3080ipx-10G es una red de conmutación Ethernet de alto ancho de banda para aplicaciones de vídeo. Este dispositivo expone una interfaz de gestión web en el puerto 80. Esta interfaz puede ser utilizada por los administradores para controlar las funciones del producto, configurar la conmutación de red y registrar licencias, entre otras funciones.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-4009 de tipo inyección de comandos que afecta a la línea de productos de Red de Vídeo Definida por Software (SDVN) de Evertz, incluyendo el 3080ipx-10G y otros dispositivos ampliamente utilizados en infraestructuras de radiodifusión, podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios del sistema como root sin autenticación, lo que supone un grave riesgo de comprometer completamente el sistema.

El componente afectado es la interfaz de administración web principal (webEASY/ewb, basada en PHP) compartida entre múltiples dispositivos Evertz.

Los archivos PHP afectados (feature-transfer-import.php, feature-transfer-export.php) crean comandos de shell directamente a partir de parámetros proporcionados por el usuario (action, filename, slot) sin una limpieza de entrada adecuada, lo que permite a los atacantes inyectar y ejecutar comandos arbitrarios.

El mecanismo de inicio de sesión login.phpse puede omitir proporcionando un JSON codificado en base64 que representa a un usuario administrador, lo que permite a los atacantes obtener acceso de administrador sin credenciales válidas.

No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- Evertz SDVN 3080ipx-10G, todas las versiones.

3. RECOMENDACIONES:

- Actualizar los paquetes afectados cuando el proveedor lance la última versión para abordar estas vulnerabilidades. Evertz no ha publicado parches ni mitigaciones a la fecha. No hay aviso ni solución oficial; la vulnerabilidad se reveló públicamente después de intentos fallidos de coordinación con Evertz.
- Aislar los dispositivos afectados de redes que no sean confiables.
- Limitar el acceso a la interfaz de administración web.
- Monitorear actividades sospechosas e intentos de acceso no autorizado.

Fuente de Información:	• hxxps://www.onekey.com/resource/security-advisory-remote-code-execution-on-evertz-svdn-cve-2025-4009 • hxxps://www.itsecuritynews.info/evertz-sdn-vulnerabilities-enable-unauthenticated-arbitrary-command-execution

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°124	Fecha: 28-05-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el servidor FTP FreeFloat		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

VulDB ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria que afecta al servidor FTP FreeFloat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario y obtener el control del sistema.

2. DETALLES:

El servidor FTP FreeFloat es un software de servidor FTP gratuito para plataformas Windows, incluyendo Windows 2000/XP y Windows CE/Pocket PC, que permite subir archivos y administrar dispositivos cableados e inalámbricos. Funciona exponiendo el puerto 21 y permite la transferencia de archivos sin requerir autenticación del usuario, lo cual puede suponer riesgos de seguridad si se utiliza en redes sin protección.

Sin embargo, se sabe que el servidor FTP FreeFloat 1.0 presenta múltiples vulnerabilidades de seguridad críticas, principalmente problemas de desbordamiento de búfer en varios controladores de comandos (como los comandos USER, PWD, MKDIR, LCD, TYPE, VERBOSE y MPUT). Estas vulnerabilidades pueden ser explotadas remotamente por atacantes para ejecutar código arbitrario o provocar una condición de denegación de servicio.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5295 de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria en el componente del controlador de comandos PORT del servidor FTP FreeFloat, podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario, lo que podría otorgar al atacante el control del sistema afectado.

La vulnerabilidad podría permitir a un atacante remoto provocar un desbordamiento de búfer mediante el envío de una entrada especialmente diseñada al controlador de comandos PORT. Una explotación exitosa puede resultar en la ejecución de código arbitrario.

El ataque puede iniciarse remotamente. El exploit se ha hecho público y está siendo utilizado por múltiples actores de amenaza para implementar malware en los dispositivos afectados.

A. Productos afectados:

- Servidor FTP FreeFloat, versión 1.0.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado cuando el proveedor lance la última versión de software disponible que aborde esta vulnerabilidad.
- Deshabilitar el servicio FTP vulnerable o restringir el acceso únicamente a hosts confiables hasta que se publique una solución que corrija esta vulnerabilidad.

Fuente de Información:	• hxxps://fitoxs.com/exploit/exploit-4f6236b59b5119d64718e994b0f3d63a755e7cb5a496e3846b92dfb960f1a80a.txt • hxxps://vuldb.com/?ctiid.310420 • hxxps://vuldb.com/?id.310420 • hxxps://vuldb.com/?submit.582988

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°124	Fecha: 28-05-2025
		Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en el servidor HTTP Apache y Tomcat en la opción Desktop Laptop (DLO) de Veritas		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Veritas Technologies ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo codificación o escape incorrectos de la salida y equivalencia de ruta: 'file.name' (punto interno) en Arctera/Veritas Desktop Laptop Option (DLO) versión 9.9 y anteriores debido a la inclusión de versiones de Apache HTTP Server y Apache Tomcat con vulnerabilidades detectadas. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-38475 de tipo codificación o escape incorrectos de la salida en mod_rewrite en Apache HTTP Server, podría permitir que un atacante asigne URL a ubicaciones del sistema de archivos que el servidor puede servir pero que no son accesibles de manera intencional o directa mediante ninguna URL, lo que resulta en la ejecución del código o la divulgación del código fuente.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo equivalencia de ruta: 'file.name' (punto interno), podría permitir a un atacante la ejecución remota de código y otros impactos en Apache Tomcat y versiones anteriores. El ataque requiere que la escritura esté habilitada para el servlet predeterminado (deshabilitado por defecto), compatibilidad con PUT parcial (habilitado por defecto) y otros conocimientos.

A. Productos afectados:

- Versiones de Arctera/Veritas Desktop Laptop Option (DLO): 9.7, 9.8, 9.8.1, 9.8.2, 9.8.3 y 9.9. Las versiones anteriores no compatibles también podrían verse afectadas.
- Servidor HTTP Apache, versiones 2.4.59 y versiones anteriores.
- Apache Tomcat 10.1.34 y versiones anteriores.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps://www.veritas.com/support/en_US/security/ARC25-007 • hxxps://www.veritas.com/support/en_US/doc/DLO_97_VxUpdate

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°124	Fecha: 28-05-2025
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Microsoft publicó actualización de Windows Server que soluciona problemas de bloqueo y reinicio de máquinas virtuales Hyper-V		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Microsoft ha lanzado una actualización de emergencia que corrige una vulnerabilidad de severidad **CRÍTICA** que provoca que algunas máquinas virtuales Hyper-V con Windows 10, Windows 11 y Windows Server se congelen o reinicien inesperadamente. Estos problemas afectan principalmente a las máquinas virtuales de Azure, que están diseñadas para proteger los datos mientras se procesan, no solo cuando se transmiten o almacenan.

2. DETALLES:

Microsoft indicó, que estas actualizaciones fuera de banda (OOB) corrigen un problema en la ruta de envío directo para una dirección física invitada (GPA) donde las máquinas virtuales confidenciales que se ejecutan en Hyper-V" podrían "dejar de responder de manera intermitente o reiniciarse inesperadamente, lo que afecta la disponibilidad del servicio y requiere intervención manual.

Este problema afecta principalmente a las máquinas virtuales confidenciales de Azure y no se espera que afecte a las implementaciones estándar de Hyper-V en el mercado, excepto en casos excepcionales que involucran una configuración de vista previa o preproducción.

Por otro lado, Microsoft indico que si aún no se ha implementado la actualización de seguridad de Windows publicados el 23 de mayo de 2025 y su entorno de TI incluye dispositivos que ejecutan Hyper-V en las versiones de Windows que se enumeran a continuación, le recomendamos que aplique esta actualización OOB en su lugar:

- Windows 11, version 24H2 (KB5061977).
- Windows Server 2025 (KB5061977).
- Windows Server 2022 (KB5061906).
- Windows 10, version 22H2 (KB5061979).
- Windows 10 Enterprise LTSC 2021 (KB5061979).
- Windows 10 Enterprise LTSC 2019 y Windows Server 2019 (KB5061978).

A. Productos afectados:

- Windows 10, Windows 11 y Windows Server.

3. RECOMENDACIÓN:

- Actualizar los productos afectados, según las publicaciones de actualizaciones OOB de Microsoft el 23 de mayo de 2025 para Windows Server 2022 (KB5061906), y el 27 de mayo de 2025 para las demás versiones de Windows afectadas. Esta actualización está disponible exclusivamente a través del Catálogo de Microsoft Update.

Fuente de Información:	• hxxps://learn.microsoft.com/en-us/windows/release-health/windows-message-center#3561 • hxxps://support.microsoft.com/es-es/topic/23-de-mayo-de-2025-kb5061906-compilaci%C3%B3n-del-so-20348-3695-fuera-de-banda-4ad7e163-1b8d-4774-bb98-d376cae6ea81 • hxxps://learn.microsoft.com/en-us/azure/confidential-computing/confidential-vm-overview • hxxps://catalog.update.microsoft.com/

Índice alfabético