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

084-2025-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°084	Fecha: 08-04-2025
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Vulnerabilidad crítica en kit de dispositivos de borde industrial		
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:

Una vulnerabilidad crítica de omisión de autenticación ha sido identificada con CVE-2024-54092 con puntuación de 9.8 en CVSS, y afecta a múltiples variantes de dispositivos Industrial Edge y dispositivos SIMATIC IPC. La vulnerabilidad se presenta en la forma en que se aplica la autenticación de usuarios en endpoints de API específicos cuando se utiliza la federación de identidades.

2. DETALLES:

Un atacante remoto no autenticado podría potencialmente:

- Evitar por completo los mecanismos de autenticación.
- Suplantar la identidad de usuarios legítimos.
- Obtener acceso no autorizado a sistemas industriales críticos.
- Potencialmente comprometer la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Para una explotación exitosa es necesario que la federación de identidad esté actualmente en uso o se haya utilizado anteriormente y que el atacante haya conocido la identidad de un usuario legítimo.

Productos afectados:

- Industrial Edge Device Kit - arm64 V1.17 (Todas las versiones).
- Industrial Edge Device Kit - arm64 V1.18 (Todas las versiones).
- Industrial Edge Device Kit - arm64 V1.19 (Todas las versiones).
- Industrial Edge Device Kit - arm64 V1.20 (Todas las versiones < V1.20.2-1).
- Industrial Edge Device Kit - arm64 V1.21 (Todas las versiones < V1.21.1-1).
- Industrial Edge Device Kit - x86-64 V1.17 (Todas las versiones).
- Industrial Edge Device Kit - x86-64 V1.18 (Todas las versiones).
- Industrial Edge Device Kit - x86-64 V1.19 (Todas las versiones).
- Industrial Edge Device Kit - x86-64 V1.20 (Todas las versiones < V1.20.2-1).
- Industrial Edge Device Kit - x86-64 V1.21 (Todas las versiones < V1.21.1-1).
- Industrial Edge Own Device (IEOD) (Todas las versiones < V1.21.1-1-a).
- Dispositivo virtual perimetral industrial (todas las versiones < V1.21.1-1-a).
- SCALANCE LPE9413 (6GK5998-3GS01-2AC2) (todas las versiones).
- Dispositivo perimetral industrial SIMATIC IPC BX-39A (todas las versiones < V3.0).
- Dispositivo perimetral industrial SIMATIC IPC BX-59A (todas las versiones < V3.0).
- Dispositivo perimetral industrial SIMATIC IPC127E (todas las versiones < V3.0).
- Dispositivo perimetral industrial SIMATIC IPC227E (todas las versiones < V3.0).
- Dispositivo perimetral industrial SIMATIC IPC427E (todas las versiones < V3.0).
- Dispositivo perimetral industrial SIMATIC IPC847E (todas las versiones < V3.0).

3. RECOMENDACIONES:

- Aplicar actualizaciones de emergencia inmediatamente en todos los dispositivos Industrial Edge y SIMATIC IPC afectados, de acuerdo a los siguientes parches disponibles:
  - Industrial Edge Device Kit arm64 V1.20.2-1 y posteriores.
  - Industrial Edge Device Kit arm64 V1.21.1-1 y posteriores.
  - Industrial Edge Device Kit x86-64 V1.20.2-1 y posteriores.
  - Industrial Edge Device Kit x86-64 V1.21.1-1 y posteriores.
  - Industrial Edge Own Device (IEOD) V1.21.1-1-a y posteriores.
  - Industrial Edge Virtual Device V1.21.1-1-a y posteriores.
  - Dispositivos SIMATIC IPC versión 3.0 y posteriores.
- Realizar una evaluación de seguridad exhaustiva de los sistemas industriales.
- Aislar los sistemas afectados si no es posible parchear.
- Deshabilitar la federación de identidad si no se requiere activamente.
- Implementar controles de mitigación temporales.
- Monitorear activamente los sistemas en busca de actividad sospechosa.
- Revisar los logs en busca de posibles compromisos.

Fuente de Información:	• hxxps://feedly.com/cve/CVE-2024-54092 • hxxps://www.cert.gov.py/actualizaciones-de-seguridad-para-productos-siemens-6/ • hxxps://www.tenable.com/cve/CVE-2024-54092 • hxxps://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/avisos-de-seguridad-de-siemens-de-abril-2025

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025
		Página: 6 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Vulnerabilidad en WhatsApp para Windows podría permitir a hackers introducir archivos maliciosos		
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:

Ha sido descubierta una vulnerabilidad en WhatsApp que puede ponerte en peligro si abres algún archivo recibido mediante WhatsApp para Windows.

2. DETALLES:

Meta ha emitido una advertencia para los usuarios de WhatsApp en Windows sobre una vulnerabilidad de seguridad que podría permitir a ciberdelincuentes disfrazar código malicioso como archivos adjuntos inofensivos. Esta vulnerabilidad ha sido registrada con el identificador CVE-2025-30401 y permite manipular la manera en que se gestionan los archivos adjuntos en la aplicación.

Normalmente, WhatsApp identifica los archivos adjuntos por su tipo MIME, lo que significa que determina el tipo de archivo - como imagen, documento o video - en función de su contenido real. Sin embargo, al momento de abrir el archivo, la aplicación se basa en la extensión del mismo, como .jpg o .exe, para decidir cómo manejarlo.

Esto puede dar lugar a confusiones si un atacante crea un desajuste intencional entre el tipo MIME y la extensión real del archivo.

El protocolo MIME (iniciales en inglés: Extensiones de Correo de Internet Multipropósito) de las comunicaciones digitales como correos electrónicos, navegadores web o aplicaciones de mensajería, es un estándar que indica la naturaleza y el formato de un archivo para que el sistema o la aplicación sepa cómo interpretarlo y manejarlo.

Por ejemplo, un archivo podría ser identificado como una imagen, mientras que su extensión indicara que se trata de un programa ejecutable.

Es decir, si alguien te envía un archivo llamado " image.jpg.exe.". WhatsApp podría mostrarlo como una imagen porque el tipo MIME indica que es una imagen. Pero si haces clic para abrirlo dentro de la aplicación, WhatsApp detectaría la terminación ".exe" y lo abriría como un programa real. Esto significa que un archivo aparentemente inofensivo podría ejecutar código malicioso sin que el usuario se dé cuenta.

Esa discordancia entre la forma en que se muestran los archivos y en lo que luego se basa WhatsApp para abrirlos es lo que podría ser aprovechado para introducir un virus o robarte tus datos, entre otras cosas, haciendo un simple clic en el archivo recibido infectado.

3. RECOMENDACIONES:

- Actualizar la aplicación a la versión 2.2450.6 o superior de WhatsApp para Windows, disponible en el sitio oficial de WhatsApp o en la Microsoft Store.
- Limitar el uso de aplicaciones personales en entornos con acceso a información sensible.
- Bloquear la ejecución automática de archivos basados solo en extensión.
- Revisar los logs de ejecución de archivos en endpoints que usen herramientas de mensajería.

Fuente de Información:	• hxxps://hackread.com/whatsapp-windows-flaw-hackers-sneak-malicious-files/ • hxxps://www.kippel01.com/tecnologia/meta-advierte-vulnerabilidad-seguridad-whatsapp-para-windows-podria-permitir-malware • hxxps://x.com/CycuraMX/status/1909648014873854327 • hxxps://www.larazon.es/tecnologia/meta-alerta-actualiza-whatsapp-evitar-esta-vulnerabilidad-seguridad-activa-2016_2025040867f578b8fd5470000128d280.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025
		Página: 7 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de omisión de verificación de imágenes del software Cisco NX-OS		
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:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo control de acceso inadecuado en el gestor de arranque del software Cisco NX-OS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la verificación de la firma de la imagen de NX-OS e instalar software no verificado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20397 de tipo control de acceso inadecuado en el gestor de arranque del software Cisco NX-OS, podría permitir que un atacante no autenticado con acceso físico a un dispositivo afectado, o un atacante local autenticado con credenciales administrativas, evite la verificación de la firma de la imagen de NX-OS.

Esta vulnerabilidad se debe a una configuración insegura del gestor de arranque. Un atacante podría explotarla ejecutando una serie de comandos del gestor de arranque. Una explotación exitosa podría permitir al atacante eludir la verificación de la firma de la imagen de NX-OS e instalar software no verificado.

Nota: Esta vulnerabilidad es relevante solo para las plataformas Cisco MDS, Nexus y UCS Fabric Interconnect que admiten la tecnología de arranque seguro.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión del software Cisco NX-OS que incluye una versión de BIOS vulnerable, independientemente de la configuración del dispositivo:

- Switches multicapa de la serie MDS 9000.
- Switches Nexus serie 3000.
- Switches Nexus serie 7000.
- Switches de red Nexus serie 9000 en modo ACI.
- Switches Nexus serie 9000 en modo NX-OS independiente.
- Interconexiones de red de la serie UCS 6400.
- Interconexiones de red de la serie UCS 6500.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025 Página: 8 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la GUI de Fortinet FortiSwitch		
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:

Fortinet, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo cambio de contraseña no verificado en la GUI de FortiSwitch. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cambiar las contraseñas de administrador sin ningún tipo de autenticación.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-48887 de tipo Cambio de contraseña no verificado, podría permitir a un atacante remoto no autenticado cambiar las contraseñas de administrador a través de una solicitud especialmente diseñada sin la verificación adecuada.

Un atacante puede cambiar de forma remota y sencilla las contraseñas administrativas de los dispositivos FortiSwitch sin necesidad de autenticación. Esto podría comprometer por completo la infraestructura de red, permitiendo el acceso no autorizado, el posible robo de datos, la manipulación de la red y la interrupción de los servicios de red.

Hasta el momento, no existen exploits conocidos públicamente para CVE-2024-48887. No se ha reportado evidencia de explotación activa ni código de prueba de concepto (PoC) disponible públicamente.

Las organizaciones que utilizan versiones afectadas de FortiSwitch deben aplicar rápidamente los parches recomendados e implementar mitigaciones para reducir los riesgos potenciales.

A. Productos afectados:

- Fortinet FortiSwitch 7.6.0.
- Fortinet FortiSwitch 7.4.0 a 7.4.4.
- Fortinet FortiSwitch 7.2.0 a 7.2.8.
- Fortinet FortiSwitch 7.0.0 a 7.0.10.
- Fortinet FortiSwitch 6.4.0 a 6.4.14.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar el acceso HTTP/HTTPS en las interfaces administrativas.
- Restringir el acceso de administración únicamente a hosts confiables.
- Aplicar las actualizaciones de seguridad proporcionadas por el proveedor lo antes posible.
- Revisar y restablecer todas las contraseñas administrativas.
- Implementar una segmentación de red adicional.
- Supervisar cualquier cambio de contraseña no autorizado o actividad de red sospechosa.

Fuente de Información:	• hxxps://fortiguard.fortinet.com/psirt/FG-IR-24-435 • hxxps://undercodenews.com/critical-fortiswitch-vulnerability-exposes-admin-passwords-what-you-need-to-know/?utm_source=feedly

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025 Página: 9 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en producto de OpenVPN		
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:

OpenVPN Inc. ha publicado una vulnerabilidad de severidad **MEDIA** de tipo comprobación inadecuada de condiciones inusuales o excepcionales que afecta a OpenVPN en modo servidor que utilizan TLS-crypt-v2. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto a realizar un ataque de denegación de servicio contra el servidor VPN mediante la reproducción de paquetes de red en la fase inicial del protocolo de enlace.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-2704 de tipo comprobación inadecuada de condiciones inusuales o excepcionales, podría permitir a un atacante remoto a realizar un ataque de denegación de servicio contra el servidor VPN mediante la reproducción de paquetes de red en la fase inicial del protocolo de enlace.

Para explotar con éxito la vulnerabilidad se requiere una clave de cliente tls-crypt-v2 válida o la observación de la red de un protocolo de enlace con una clave de cliente tls-crypt-v2 válida.

Este error no afecta a los clientes OpenVPN. No afecta a los servidores OpenVPN 2.4 o 2.5, ni a los servidores OpenVPN 2.6 que se ejecutan sin --tls-crypt-v2.

A. Productos afectados:

- OpenVPN versiones: 2.6.1 hasta la 2.6.13.
- Sistemas operativos afectados; Ubuntu, suse, Red Hat, Debian.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//community[.]openvpn[.]net/openvpn/wiki/CVE-2025-2704. • hxxp://www.openwall.com/lists/oss-security/2025/04/02/5

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025
		Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en módulo de Apache		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo deserialización de datos no confiables que afecta a la biblioteca Java Apache Parquet, específicamente en el módulo parquet-avro. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-30065 de tipo deserialización de datos no confiables, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad explota el campo default en los esquemas de Avro, lo que permite la instanciación de clases Java arbitrarias. Esto permite a los atacantes ejecutar código malicioso si un sistema vulnerable deserializa un esquema creado y tiene la clase de carga útil objetivo en su ruta de clases.

A. Productos afectados:

- Apache Parquet Java: 1.0.0-t1 - 1.15.1 rc0.

B. Prueba de concepto (PoC)

Se ha publicado en GitHub una prueba de concepto (PoC) para CVE-2025-30065, que demuestra cómo se puede explotar la vulnerabilidad generando un archivo Parquet malicioso. Esta PoC está destinada únicamente a fines educativos y de investigación de seguridad autorizada.

 # Get Parquet Avro dependency
mvn dependency:get -Dartifact=org.apache.parquet:parquet-avro:1.15.0

 # Compile
Javac –cp ~/.m2/repository/org/apache/parquet/*:~/.m2/repository/org/apache/hadoop
/* ParquetExploitGenerator.java

 # Run
java -cp .:~/.m2/repository/org/apache/parquet/*:~/.m2/repository/org/apache/hadoop
/* ParquetExploitGenerator

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/04/01/1; • hxxp[:]//lists[.]apache[.]org/thread/okzqb3kn479gqzxm21gg5vqr35om9gw5; • hxxps[:]//github[.]com/h3st4k3r/CVE-2025-30065.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°084	Fecha: 08-04-2025
		Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos de Fortinet		
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 **MEDIA** de tipo secuencias de comandos entre sitios (XSS) que afecta a Fortinet FortiClient. La explotación exitosa de esta vulnerabilidad podría permitir a un administrador de EMS enviar mensajes que pueden ejecutar código JavaScript malicioso en las versiones afectadas.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-22855 de tipo secuencias de comandos entre sitios, podría permitir a un administrador de EMS enviar mensajes que pueden ejecutar código JavaScript malicioso en las versiones afectadas.

Esta vulnerabilidad implica una neutralización incorrecta de la entrada durante la generación de páginas web, lo que provoca un problema de XSS. Podría permitir que un administrador de EMS envíe mensajes que pueden ejecutar JavaScript malicioso en las versiones afectadas.

A. Productos afectados:

- FortiClientEMS versiones 7.4.0 hasta la 7.4.1.
- FortiClientEMS versiones 7.2.1 hasta la 7.2.8.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//fortiguard[.]Fortinet[.]com/psirt/FG-IR-23-344

Índice alfabético