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

100-2025-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°100	Fecha: 29-04-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los usuarios de WooCommerce son blanco de una campaña de phishing		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Una nueva campaña de phishing a gran escala está atacando a administradores de WooCommerce con correos falsos de "alerta crítica", instándolos a instalar un parche de seguridad que en realidad añade puertas traseras en sus sitios WordPress.

2. DETALLES:

Investigadores de la empresa de seguridad de WordPress Patchstack detectaron que, al descargar el supuesto parche, las víctimas instalan un plugin malicioso que:

- Crea un administrador oculto en el sitio web.
- Descarga cargas útiles de tipo web Shell.
- Mantiene acceso persistente para los atacantes.

Esta operación parece ser la continuación de una campaña similar detectada en 2023, reutilizando técnicas idénticas de camuflaje de cargas y plantillas de correo.

Así opera la estafa:

- Los correos se envían desde help@security-woocommerce[.]com, simulando ser WooCommerce.
- Aseguran que el sitio está en riesgo por una supuesta vulnerabilidad de “acceso administrativo no autenticado”.
- Urgen a instalar un "parche crítico" a través de un botón en el correo.
- Redirigen a una página fraudulenta usando un dominio homógrafo: woocommėrce[.]com (empleando una "ė" en lugar de una "e").

Acciones tras la infección:

- Se crea un cronjob que intenta generar un nuevo usuario admin cada minuto.
- Se establece conexión con woocommerce-services[.]com para descargar una segunda carga maliciosa.
- Se instalan varios webs shells como P.A.S.-Form, p0wny y WSO en la carpeta de cargas de WordPress.

Estas puertas traseras permiten: Control total del sitio, inyección de anuncios maliciosos, redirección de visitantes, robo de datos de tarjetas de pago, integración del servidor a redes de DDoS o incluso cifrado de archivos para extorsión (ransomware), etc. Además, el plugin se oculta automáticamente de la lista de plugins activos y oculta la cuenta de administrador creada.

3. RECOMENDACIONES:

- No abrir archivos adjuntos ni enlaces presentes en correos electrónicos sospechosos ni en otros mensajes, ni descargar desde sitios que no sean oficiales.
- Revisar la existencia de cuentas admin con nombres aleatorios de 8 caracteres.
- Buscar cronjobs sospechosos.
- Analizar tráfico saliente hacia woocommerce-services[.]com, woocommerce-api[.]com o woocommerce-help[.]com.

Fuente de Información:	• hxxps://thehackernews.com/2025/04/woocommerce-users-targeted-by-fake.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°100	Fecha: 29-04-2025 Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Mozilla Firefox y Firefox para Android		
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 **ALTA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria que afecta a Mozilla Firefox y Firefox para Android. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-4092 de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria que afecta a Mozilla Firefox y Firefox para Android, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de límite al procesar contenido HTML. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar corrupción de memoria y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

A. Productos afectados:

- Mozilla Firefox: 130.0 - 137.0.2.
- Firefox para Android: 130.0 - 137.0.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.mozilla.org/en-US/security/advisories/mfsa2025-28/ • hxxps://www.mozilla.org/security/advisories/mfsa2025-31/ • hxxps://bugzilla.mozilla.org/buglist.cgi?bug_id=1924108%2C1950780%2C1959367

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°100	Fecha: 29-04-2025
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la biblioteca Apache Commons Compress en productos IBM		
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 Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo Denegación de servicio (DoS) por error de falta de memoria relacionada con la biblioteca Apache Commons Compress que afecta específicamente a IBM WebSphere Application Server Liberty y productos de IBM relacionados. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de DoS.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2021-33517 de tipo denegación de servicio por error de falta de memoria, podría permitir a un atacante remoto realizar un ataque de DoS.

Esta vulnerabilidad consiste en un problema de DoS causado por un error de memoria insuficiente al procesar archivos TAR especialmente diseñados. Un atacante puede explotar esto persuadiendo a la víctima para que abra un archivo TAR malicioso, lo que provoca que la aplicación asigne memoria excesiva, lo que genera una condición de denegación de servicio en los servicios que utilizan el paquete tar de Apache Commons Compress.

A. Productos afectados:

- IBM Business Automation Workflow versiones V18.0, V19.0, V20.0 y V21.0.
- IBM Business Process Manager versiones 8.5 y 8.6.
- IBM WebSphere Application Server Liberty versiones 17.0.0.3 a 21.0.0.9.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Aplicar parches y actualizaciones de seguridad de IBM según los boletines de seguridad de IBM.

Fuente de Información:	• hxxps[:]//www[.]ibm[.]com/support/pages/node/6556922

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°100	Fecha: 29-04-2025 Página: 7 de 9

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

Apple Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desreferencia de puntero nulo que afecta a las plataformas Apple. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24179 de tipo desreferencia de puntero nulo, podría permitir a un atacante remoto realizar un ataque de DoS. Esto podría interrumpir el funcionamiento normal del dispositivo o causar inestabilidad en las aplicaciones afectadas.

La vulnerabilidad existe debido a un error de desreferencia de puntero nulo en AirPlay. Un atacante remoto en la red local puede enviar paquetes especialmente diseñados al dispositivo y realizar un ataque de denegación de servicio o la finalización inesperada de la aplicación.

A. Productos afectados:

- iOS 18.2 y anteriores.
- iPadOS 18.2 y anteriores.
- visionOS anterior a 2.3.
- macOS Ventura 13.7.5.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Apple corrigió esta vulnerabilidad mejorando la validación de entrada para evitar la desreferencia de puntero nulo. La corrección se ha incorporado a las actualizaciones de iOS 18.3, iPadOS 18.3, visionOS 2.3 y macOS Ventura 13.7.5.

Fuente de Información:	• hxxps[:]//support[.]apple[.]com/en-us/122066 • hxxps[:]//support[.]apple[.]com/en-us/122068 • hxxps[:]//support[.]apple[.]com/en-us/122072 • hxxps[:]//support[.]apple[.]com/en-us/122073 • hxxps[:]//support[.]apple[.]com/en-us/122372 • hxxps[:]//support[.]apple[.]com/en-us/122374 • hxxps[:]//support[.]apple[.]com/en-us/122375

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°100	Fecha: 29-04-2025 Página: 8 de 9

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

Meta Platforms, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo escritura fuera de límites en FreeType que afecta específicamente a las versiones 2.13.0 y anteriores. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema objetivo y comprometer el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27363 de tipo escritura fuera de límites en FreeType, podría permitir a un atacante remoto comprometa el sistema vulnerable. La vulnerabilidad existe debido a un error de límite al procesar entradas no confiables. Un atacante remoto puede pasar una fuente especialmente diseñada a la aplicación que usa una versión afectada de la biblioteca, activar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- FreeType: 1.3.1, anterior a 2.13.0.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Mantener bibliotecas de representación de fuentes actualizadas en sistemas expuestos a archivos de fuentes no confiables.

Fuente de Información:	• hxxps[:]//www[.]Facebook[.]com/security/advisories/cve-2025-27363 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/1 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/2 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/3 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/8 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/11 • hxxps[:]//www[.]openwall[.]com/lists/oss-security/2025/03/13/12

Índice alfabético