



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

## 041-2026-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 Aérea del 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 las empresas 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

Red Hat advierte sobre malware incrustado en una popular herramienta de Linux, lo que abre las puertas al acceso no autorizado. .... 4

Vulnerabilidad en componentes de Apple. .... 6

Vulnerabilidad en el software Cisco IOS XE Wireless Controller. .... 7

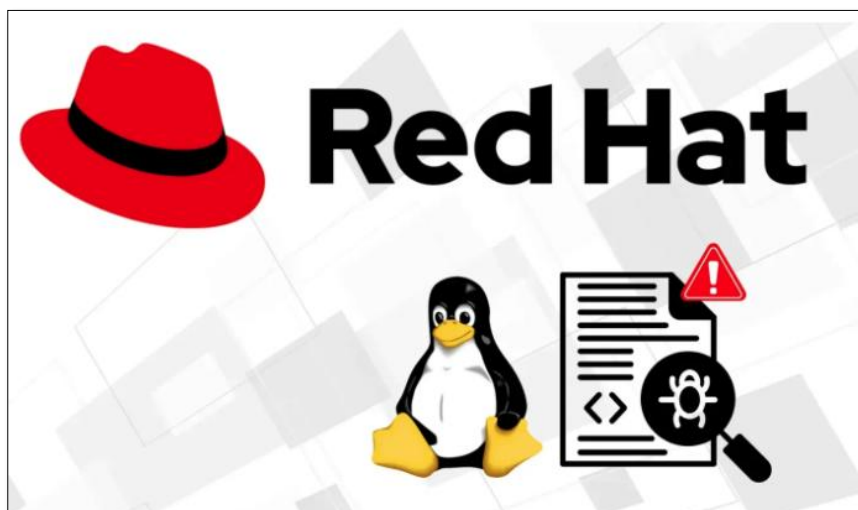
Índice alfabético ..... 8

 Centro Nacional de Seguridad Digital	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°041</b>		Fecha: 27-03-2026
			Página: 4 de 8
<b>Componente que reporta</b>	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
<b>Nombre de la alerta</b>	Red Hat advierte sobre malware incrustado en una popular herramienta de Linux, lo que abre las puertas al acceso no autorizado.		
<b>Tipo de Ataque</b>	Malware	<b>Abreviatura</b>	Malware
<b>Medios de propagación</b>	USB, Disco, Red, Correo, Navegación de Internet		
<b>Código de familia</b>	C	<b>Código de Sub familia</b>	C02
<b>Clasificación temática familia</b>	Código Malicioso		

**Descripción**

**1. ANTECEDENTES:**

Red Hat emitió una alerta crítica tras identificarse un ataque altamente sofisticado contra la cadena de suministro de software libre, dirigido a XZ Utils, una herramienta de compresión ampliamente utilizada en sistemas Linux. Investigadores de seguridad descubrieron que versiones recientes de las bibliotecas xz y xz-libs contenían código malicioso oculto, lo que representa un riesgo severo debido a la ubicuidad de este componente en entornos comunitarios y empresariales. Este incidente pone de manifiesto la creciente tendencia de los actores de amenaza a comprometer proyectos de código abierto confiables para distribuir malware de forma silenciosa y masiva, evadiendo revisiones tradicionales y controles de integridad en el código fuente.



*Ilustración 1: Red Hat ha emitido una alerta de seguridad*

**2. DETALLES:**


La vulnerabilidad, identificada como CVE-2024-3094, afecta a las versiones 5.6.0 y 5.6.1 de XZ Utils. El código malicioso fue cuidadosamente ofuscado y no está presente de forma visible en el repositorio Git principal. En su lugar, se activa durante el proceso de compilación mediante una macro M4 oculta, ensamblando el payload final solo en los paquetes oficiales distribuidos. Una vez instalada, la librería comprometida interfiere con el proceso de autenticación de sshd a través de systemd, permitiendo, bajo ciertas condiciones, eludir los mecanismos de autenticación SSH. Esto podría otorgar a un atacante acceso remoto completo y persistente al sistema afectado. Los entornos impactados incluyen Fedora Rawhide, Fedora 40 Beta, Debian unstable (Sid) y openSUSE, mientras que Red Hat Enterprise Linux (RHEL) no se encuentra afectado según las evaluaciones actuales.


- **RECOMENDACIONES:**

- Revertir inmediatamente XZ Utils a versiones seguras 5.4.x en todos los sistemas potencialmente afectados.
- Evitar el uso de distribuciones beta o inestables en entornos productivos o críticos.
- Implementar verificación de integridad y firma de paquetes en pipelines de CI/CD.
- Fortalecer la segmentación de red y el control de acceso SSH, incluyendo autenticación multifactor.
- Monitorear logs del sistema y de sshd en búsqueda de intentos de autenticación anómalos o accesos inesperados.
- Incorporar escaneo de dependencias y análisis de cadena de suministro (SCA) en procesos DevSecOps.
- Mantener actualizadas las listas de inteligencia de amenazas y alertas de proveedores oficiales (Red Hat, Fedora, Debian).
- Aplicar el principio de mínimo privilegio en cuentas de administración y servicios.
- Establecer planes de respuesta ante incidentes de supply chain, incluyendo validación forense y reinstalación confiable si se detecta compromiso.

Fuente de Información:

- <https://gbhackers.com/red-hat-warns-of-malware-embedded-in-popular-linux-tool/>

	<b>ALERTA DE SEGURIDAD DIGITAL N°178</b>		Fecha: 27-03-2026
			Página: 6 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad en componentes de Apple.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Apple Inc. ha publicado una vulnerabilidad de severidad <b>ALTA</b> clasificada como CWE-667: bloqueo incorrecto en el componente XNU del kernel de Apple que afecta iOS, iPadOS, macOS y demás plataformas Apple. La explotación exitosa de esta vulnerabilidad podría permitir a una aplicación maliciosa modificar inesperadamente la memoria compartida entre procesos.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>alta</b> identificada por MITRE como <a href="#">CVE-2025-43510</a> de tipo CWE-667: bloqueo incorrecto en el componente XNU del kernel de Apple que afecta iOS, iPadOS, macOS y demás plataformas Apple, podría permitir a una aplicación maliciosa modificar inesperadamente la memoria compartida entre procesos. En la cadena DarkSword, explotada como bug de copy-on-write en el proceso mediaplaybackd para construir primitivas de ejecución arbitraria. Actualizar a iOS/iPadOS 18.7.2 o iOS/iPadOS 26.1.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– macOS Tahoe versiones anteriores a 26.1 (“Tahoe+8” en algunos resúmenes).</li> <li>– macOS Sequoia versiones anteriores a 15.7.2.</li> <li>– macOS Sonoma versiones anteriores a 14.8.2.</li> <li>– iOS versiones anteriores a 18.7.2.</li> <li>– iPadOS versiones anteriores a 18.7.2 y también anterior a 26.1 en algunas cadenas.</li> <li>– tvOS versiones anteriores a 26.1.</li> <li>– visionOS versiones anteriores a 26.1.</li> <li>– watchOS versiones anteriores a 26.1.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Actualizar el producto afectado a la última versión de software disponible que corrige esta vulnerabilidad.</li> <li>• Habilitar y revisar logs de seguridad del sistema (Apple System Log, Unified Logging) y soluciones EDR para detectar anomalías en el kernel, procesos GPU o WebContent.</li> <li>• Bloquear o inspeccionar tráfico a dominios o IPs conocidas por alojar exploits DarkSword, apoyándose en feeds de threat-intelligence (Google TAG, iVerify, etc.)</li> </ul>			
<b>Fuente de Información:</b>	<ul style="list-style-type: none"> <li>• <a href="https://support.apple.com/en-us/125634">hxxps[:]//support[.]apple[.]com/en-us/125634</a></li> <li>• <a href="https://support.apple.com/en-us/125636">hxxps[:]//support[.]apple[.]com/en-us/125636</a></li> <li>• <a href="https://support.apple.com/en-us/125638">hxxps[:]//support[.]apple[.]com/en-us/125638</a></li> </ul>		

	<b>ALERTA DE SEGURIDAD DIGITAL N°179</b>		<b>Fecha: 27-03-2026</b>
			<b>Página: 7 de 8</b>
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad en el software Cisco IOS XE Wireless Controller.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	USB, Disco, Red, Correo, Navegación de Internet		
<b>Código de familia</b>	C	<b>Código de Sub familia</b>	C03
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Cisco Systems, Inc. ha reportado una vulnerabilidad de severidad <b>ALTA</b> clasificada como CWE-230: Manejo inadecuado de valores faltantes en el procesamiento de los paquetes de Control y Aprovisionamiento de Puntos de Acceso Inalámbricos (CAPWAP) del software Cisco IOS XE Wireless Controller para la familia Catalyst CW9800. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto no autenticado provoque una denegación de servicio (DoS) en un dispositivo afectado.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>alta</b> identificada por MITRE como <a href="#">CVE-2026-20086</a> en el procesamiento de los paquetes de Control y Aprovisionamiento de Puntos de Acceso Inalámbricos (CAPWAP) del software Cisco IOS XE Wireless Controller para la familia Catalyst CW9800 podría permitir que un atacante remoto no autenticado provoque una denegación de servicio (DoS) en un dispositivo afectado.</p> <p>Esta vulnerabilidad se debe a un manejo inadecuado de un paquete CAPWAP mal formado. Un atacante podría explotarla enviando un paquete CAPWAP mal formado a un dispositivo afectado. Si la explotación es exitosa, el atacante podría provocar que el dispositivo afectado se reinicie inesperadamente, lo que resultaría en una DoS.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE Wireless Controller, independientemente de la configuración del dispositivo: Controladores inalámbricos Catalyst CW9800H, Controladores inalámbricos Catalyst CW9800M.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas para corregirla.</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li>• <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm</a></li> </ul>	

## Índice alfabético

Malware ..... 4

Explotación de vulnerabilidades conocidas ..... 6,7