



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

042-2026-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

Se abusa de herramientas de Windows para desactivar el antivirus antes de ataques de ransomware. 4

Vulnerabilidad en Cisco IOS Software y Cisco IOS XE Software Release 3E con la característica HTTP Server habilitada. 6

Índice alfabético 8

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°042		Fecha: 30-03-2026
			Página: 4 de 8
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Se abusa de herramientas de Windows para desactivar el antivirus antes de ataques de ransomware.		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Investigaciones recientes publicadas por GBHackers alertan sobre una tendencia creciente en la que actores de amenazas están abusando de herramientas nativas y legítimas de Windows para preparar el terreno antes de ejecutar ataques de alto impacto, como ransomware. En lugar de introducir malware evidente, los atacantes aprovechan utilidades confiables incluidas en el sistema operativo para deshabilitar antivirus y soluciones EDR, reduciendo la probabilidad de detección. Este enfoque, conocido como Living-off-the-Land, refleja una evolución en las tácticas de intrusión, donde la evasión y el sigilo son prioritarios frente a la explotación directa, incrementando la efectividad de ataques dirigidos y de rápida ejecución.



Ilustración 1: Los piratas informáticos están convirtiendo cada vez más las herramientas legítimas

2. DETALLES:


Según el reporte, los atacantes emplean herramientas administrativas de Windows como PowerShell, cmd.exe, net.exe, sc.exe y utilidades de administración de servicios para detener procesos de seguridad, modificar políticas y desactivar mecanismos de protección en tiempo real. Estas acciones suelen realizarse tras obtener acceso inicial, permitiendo neutralizar defensas sin desplegar binarios maliciosos visibles. Debido a que estas herramientas son legítimas, firmadas por Microsoft y comúnmente usadas por administradores, su actividad se confunde con operaciones normales del sistema. Una vez que las soluciones de seguridad han sido degradadas o eliminadas, los atacantes lanzan la fase final del ataque, frecuentemente un despliegue de ransomware, con una tasa de éxito significativamente mayor y tiempos de respuesta más cortos para las víctimas.

- **RECOMENDACIONES:**

- Implementar EDR/XDR con detección basada en comportamiento, no solo en firmas, para identificar abuso de LOLBins.
- Restringir el uso de PowerShell mediante Constrained Language Mode y aplicar ejecución firmada únicamente.
- Habilitar registro avanzado y auditoría de comandos administrativos (PowerShell Logging, AMSI, Sysmon).
- Aplicar el principio de mínimo privilegio y separar cuentas administrativas de cuentas de usuario final.
- Monitorear eventos asociados a detención o desinstalación de herramientas de seguridad como indicadores críticos.
- Integrar controles de Application Control (WDAC / AppLocker) para limitar uso indebido de binarios del sistema.
- Mantener playbooks de respuesta que contemplen ataques fileless y LOLBins, integrados con SOAR.
- Capacitar a equipos SOC y TI en la detección temprana de tácticas previas a ransomware y cadenas de ataque.

Fuente de Información:

- <https://gbhackers.com/windows-tools-abused/>

	ALERTA DE SEGURIDAD DIGITAL N°180		Fecha: 30-03-2026
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Cisco IOS Software y Cisco IOS XE Software Release 3E con la característica HTTP Server habilitada.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Cisco ha reportado una vulnerabilidad de severidad ALTA clasificada como CWE-228: Manejo Impropio de Estructura Sintácticamente Inválida que afecta a Cisco IOS Software y Cisco IOS XE Software Release 3E con la característica HTTP Server habilitada. Esta vulnerabilidad representa un riesgo significativo para las organizaciones que utilizan estos sistemas operativos de red, ya que permite a un atacante remoto autenticado causar el reinicio inesperado del dispositivo afectado, resultando en una condición de denegación de servicio (DoS) que interrumpe la disponibilidad de servicios de red críticos.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad alta identificada por MITRE como CVE-2026-20125 reside específicamente en la funcionalidad HTTP Server de Cisco IOS e IOS XE Release 3E, donde el software no valida adecuadamente la entrada proporcionada por el usuario al procesar solicitudes HTTP. Cuando un atacante envía solicitudes HTTP malformadas al dispositivo, el código del servidor HTTP no logra detectar y rechazar apropiadamente las estructuras sintácticamente inválidas. Esta falla en la validación de entrada permite que datos maliciosos lleguen a rutinas internas de procesamiento que no pueden manejar adecuadamente dichas estructuras, provocando una inestabilidad del sistema que activa el mecanismo de "watchdog timer".</p> <p>El watchdog timer es un mecanismo de hardware o software diseñado para monitorear la salud del sistema y reiniciar el dispositivo si detecta que el sistema se ha vuelto no responsivo. En este caso, la solicitud HTTP malformada desencadena una condición que causa la expiración prematura del watchdog timer, forzando un reinicio completo del dispositivo. Este reinicio resulta en la pérdida temporal de todos los servicios de red proporcionados por el dispositivo afectado, incluyendo enrutamiento, switching y cualquier función de gestión de red activa. La vulnerabilidad es particularmente preocupante porque puede ser explotada repetidamente para mantener una condición de denegación de servicio persistente.</p> <p>Según el equipo Cisco PSIRT (Product Security Incident Response Team), no se tiene conocimiento de anuncios públicos o uso malicioso de esta vulnerabilidad en el momento de la publicación del aviso. No existe un PoC (Proof of Concept) públicamente disponible documentado.</p> <p>La explotación requiere que el atacante posea una cuenta de usuario válida en el dispositivo objetivo, lo que reduce el riesgo de explotación masiva pero no elimina la amenaza de insiders maliciosos o atacantes que hayan comprometido credenciales previamente.</p> <p>Las organizaciones enfrentan un riesgo operativo significativo debido al papel crítico que desempeñan los dispositivos Cisco IOS en la infraestructura de red. Aunque el requisito de autenticación reduce la probabilidad de explotación por actores de amenaza externos no autorizados, el riesgo de insiders maliciosos, cuentas comprometidas, o atacantes que hayan obtenido credenciales mediante phishing u otros medios permanece elevado. Entornos con múltiples administradores de red, contratistas con acceso temporal, o políticas de contraseñas débiles son particularmente vulnerables. El riesgo se magnifica en arquitecturas donde un único dispositivo afectado podría causar una interrupción en cascada a través de la red.</p> <p>La recomendación técnica prioritaria es implementar controles de acceso estrictos al HTTP Server, considerar el uso de gestión fuera de banda, y aplicar las actualizaciones de Cisco tan pronto como sea operativamente factible. La capacidad de deshabilitar completamente el HTTP Server como workaround proporciona una opción de mitigación inmediata para organizaciones que no dependan de la gestión web de sus dispositivos.</p>			

A. Productos afectados:

- Cisco IOS Software con la característica HTTP Server habilitada (múltiples versiones 12.x y 15.x).
- Cisco IOS XE Software Release 3E con la característica HTTP Server habilitada.

B. Indicadores de Compromiso (IoC):

- Reinicios inesperados y no programados del dispositivo Cisco IOS/IOS XE.
- Eventos de expiración del watchdog timer registrados en los logs del dispositivo.
- Patrones inusuales de solicitudes HTTP desde usuarios autenticados dirigidas a la interfaz de gestión.
- Múltiples eventos de reinicio en sucesión rápida indicando intentos de explotación potenciales.
- Mensajes de error relacionados con el módulo WEB_EXEC en los logs del servidor HTTP.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que corrige esta vulnerabilidad.
- Si no es operativamente requerido, deshabilitar la característica HTTP Server usando los comandos: no ip http server / no ip http secure-server.
- Implementar listas de control de acceso (ACLs) para limitar el acceso HTTP/HTTPS a interfaces de gestión desde direcciones IP de confianza únicamente: access-list 10 permit 10.10.10.0 0.0.0.255 / ip http access-class 10.
- Utilizar redes de gestión fuera de banda (out-of-band) para aislar el tráfico de gestión de dispositivos de las redes de producción.
- Habilitar Control Plane Policing (CoPP) para limitar la tasa de tráfico HTTP dirigido al dispositivo.
- Revisar y auditar cuentas de usuario con acceso HTTP Server, eliminando privilegios innecesarios.
- Configurar SNMP traps o alertas syslog para eventos de reinicio del dispositivo y habilitar logging detallado del HTTP Server.

Fuente de Información:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-dos-sbv8XRpL>

Índice alfabético

Ransomware 4

Explotación de vulnerabilidades conocidas 6