



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

044-2026-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

Instaladores falsos propagan troyanos de acceso remoto (RAT) y mineros de Monero en una campaña de malware en curso.....	4
Vulnerabilidad crítica en Cisco Smart Software Manager On-Prem.....	6
Vulnerabilidad crítica en Fortinet FortiClientEMS.....	7
Índice alfabético	8

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°044		Fecha: 06-04-2026
			Página: 4 de 8
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Instaladores falsos propagan troyanos de acceso remoto (RAT) y mineros de Monero en una campaña de malware en curso.		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El uso de software fraudulento como vector de infección es una técnica recurrente que ha evolucionado significativamente en los últimos años. Los atacantes aprovechan la confianza de los usuarios en aplicaciones populares y en descargas aparentemente legítimas para introducir malware avanzado en los sistemas. En este contexto, campañas recientes han demostrado un incremento en el uso de instaladores falsificados que imitan herramientas conocidas, combinando ingeniería social, abuso de repositorios confiables y técnicas de evasión para comprometer equipos sin generar alertas inmediatas. Este escenario representa un riesgo alto para la confidencialidad, integridad y control de los sistemas afectados



Ilustración 1 En una operación de malware de larga duración, se están utilizando instaladores de software falsos para distribuir troyanos de acceso remoto (RAT)

2. DETALLES:

La investigación reveló una campaña maliciosa que utiliza instaladores falsos de software popular distribuidos a través de sitios web fraudulentos y páginas de phishing que simulan portales oficiales. Estos instaladores, generalmente en formato MSI, ejecutan simultáneamente componentes legítimos para no levantar sospechas y cargas maliciosas ocultas mediante técnicas como DLL sideloading.


El malware principal identificado corresponde al Sainbox RAT, una variante de Gh0stRAT, que otorga control remoto total al atacante, permitiendo robo de información, ejecución de comandos y despliegue de payloads adicionales. Adicionalmente, se incorpora un rootkit a nivel kernel basado en el proyecto Hidden, diseñado para ocultar procesos, archivos y claves de registro, incrementando la persistencia y evadiendo soluciones de seguridad. La campaña muestra un nivel técnico elevado, enfocado en mantener sigilo, persistencia y control prolongado del sistema comprometido.


3. RECOMENDACIONES:

- Descargar software exclusivamente desde sitios oficiales o repositorios corporativos verificados.
- Implementar soluciones EDR/XDR con detección de RATs, DLL sideloading y rootkits.
- Restringir la ejecución automática de archivos MSI y DLL desde ubicaciones no confiables.
- Aplicar principios de Zero Trust a la instalación y ejecución de software.
- Monitorear la creación de claves de inicio automático y servicios persistentes en el sistema.
- Mantener listas de aplicaciones permitidas (Application Allowlisting).
- Capacitar a los usuarios sobre riesgos de instaladores falsos y sitios clonados.
- Actualizar de forma continua el sistema operativo y drivers para reducir abuso de componentes vulnerables.
- Inspeccionar tráfico saliente en busca de comportamientos de C2 típicos de RATs.

Fuente de Información:

- <https://gbhackers.com/fake-installers-spread-rats/>

	ALERTA DE SEGURIDAD DIGITAL N°182		Fecha: 06-04-2026
			Página: 6 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Cisco Smart Software Manager On-Prem.		
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 Systems, Inc. ha reportado una vulnerabilidad de severidad CRÍTICA identificada como CWE-668: Exposición de recursos a la esfera equivocada en Cisco Smart Software Manager On-Prem (SSM On-Prem). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de un host SSM On-Prem afectado.</p> <p>La vulnerabilidad puede provocar la interrupción de servicios de red esenciales, afectando routers y switches críticos. Esto puede generar pérdida de conectividad, interrupción de servicios empresariales y degradación de operaciones en infraestructuras dependientes de red.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-20160 en Cisco Smart Software Manager On-Prem (SSM On-Prem) podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de un host SSM On-Prem afectado.</p> <p>Esta vulnerabilidad se debe a la exposición involuntaria de un servicio interno. Un atacante podría explotarla enviando una solicitud manipulada a la API del servicio expuesto. Una explotación exitosa podría permitir al atacante ejecutar comandos en el sistema operativo subyacente con privilegios de administrador.</p> <p>La vulnerabilidad puede provocar la interrupción de servicios de red esenciales, afectando routers y switches críticos. Esto puede generar pérdida de conectividad, interrupción de servicios empresariales y degradación de operaciones en infraestructuras dependientes de red.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Esta vulnerabilidad afecta a Cisco SSM On-Prem, independientemente de la configuración del software. <p>B. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – Reinicios inesperados de dispositivos de red. – Caída de servicios de routing o switching. – Tráfico anómalo dirigido a puertos o servicios específicos. – Logs con errores relacionados a procesamiento de paquetes. – Incremento de paquetes malformados en análisis de red. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Cisco ha publicado actualizaciones de software que solucionan esta vulnerabilidad. No existen soluciones alternativas para corregirla. • Filtrar tráfico de red no confiable en perímetros. • Implementar ACLs para restringir acceso a servicios críticos. • Monitorear tráfico y eventos de red en tiempo real. • Deshabilitar servicios innecesarios expuestos. 			
Fuente de Información:	<ul style="list-style-type: none"> • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-CHUcWuNr 		

	ALERTA DE SEGURIDAD DIGITAL N°183		Fecha: 06-04-2026
			Página: 7 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Fortinet FortiClientEMS.		
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>Fortinet, Inc. ha reportado una vulnerabilidad de severidad CRÍTICA clasificada como CWE-284: Control de acceso inadecuado que afecta a Fortinet FortiClientEMS la cual permite a un atacante remoto no autenticado eludir mecanismos de autenticación y obtener acceso privilegiado al sistema, comprometiendo completamente la confidencialidad, integridad y disponibilidad de la infraestructura afectada.</p> <p>El riesgo es crítico, especialmente para organizaciones que exponen dispositivos Fortinet a Internet. Este tipo de vulnerabilidad es altamente atractivo para actores APT y grupos de ransomware, ya que proporciona acceso directo a dispositivos perimetrales clave.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad crítica identificada por MITRE como CVE-2026-35616 se origina en una validación incorrecta de las solicitudes HTTP/HTTPS hacia la interfaz de administración, donde ciertos encabezados o parámetros pueden ser manipulados para evadir los controles de autenticación. Esto permite que un atacante acceda a endpoints administrativos sin proporcionar credenciales válidas.</p> <p>A nivel técnico, el fallo radica en la lógica de autorización, donde el sistema no valida adecuadamente el contexto de sesión o confía en datos controlables por el usuario. Esto posibilita la ejecución de acciones administrativas, como modificación de configuraciones, creación de usuarios o alteración de políticas de seguridad, sin necesidad de autenticación previa.</p> <p>La explotación permite el acceso total al sistema, incluyendo la capacidad de modificar reglas de firewall, interceptar tráfico, deshabilitar controles de seguridad y establecer persistencia. Esto puede derivar en compromisos completos de red y facilitar movimientos laterales dentro de la infraestructura.</p> <p>Hasta el momento, no se ha confirmado explotación activa a gran escala; sin embargo, vulnerabilidades similares en productos Fortinet han sido históricamente explotadas rápidamente por actores de amenaza. Existen reportes preliminares de pruebas de concepto (PoC) que demuestran la evasión de autenticación, lo que incrementa el riesgo de explotación en entornos expuestos a Internet.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> – Fortinet FortiClientEMS, versión 7.4.5 a 7.4.6. <p>B. Indicadores de Compromiso (IoC):</p> <ul style="list-style-type: none"> – Accesos no autorizados a la interfaz administrativa. – Creación de cuentas administrativas desconocidas. – Cambios inesperados en configuraciones de firewall. – Logs con sesiones autenticadas sin credenciales válidas. – Tráfico HTTP/HTTPS anómalo hacia endpoints de administración. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Aplicar parches de seguridad publicados por Fortinet. • Restringir acceso a interfaces de administración (VPN / IP whitelist). • Habilitar autenticación multifactor (MFA). • Monitorear logs de autenticación y configuración. • Deshabilitar exposición directa de interfaces administrativas a Internet. 			
Fuente de Información:		<ul style="list-style-type: none"> • hxxps://www.fortiguard.com/psirt/FG-IR-26-099 • https://fortiguard.fortinet.com/psirt/FG-IR-26-099 	

Índice alfabético

Malware 4

Explotación de vulnerabilidades conocidas 6,7