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

280-2024-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°280	Fecha: 04-12-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ransomware FOG activo en América Latina		
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:

Se ha detectado un ransomware conocido como "The Fog", una variante de STOP/DJVU que anteriormente atacaba sectores educativos y recreativos, pero ahora se dirige a la industria financiera.

El ransomware Fog surgió en abril de 2024 con operaciones dirigidas a sistemas Windows y Linux. Fog es una operación de extorsión de múltiples frentes que aprovecha un Dedicated Leak Sites (DLS). basado en TOR para enumerar a las víctimas y alojar datos de quienes se niegan a cumplir con sus demandas de rescate.

En agosto de 2024, los ciberdelincuentes usaron credenciales de VPN comprometidas para lanzar un ataque contra una institución financiera mediana, utilizando "Fog" (también llamado “Lost in the Fog”) para comprometer datos en sistemas Windows y Linux.

2. DETALLES:

Los actores de amenazas Fog dependen en gran medida de la explotación de aplicaciones conocidas y vulnerables. Los operadores generalmente logran el acceso inicial mediante la compra de credenciales comprometidas de un Agente de Acceso Inicial (IAB). Los operadores aprovecharán cuentas comprometidas y/o compradas en el mercado negro para establecer un punto de apoyo en el entorno y luego se mueven lateralmente de manera metódica.

Existen variantes del ransomware Fog para plataformas Windows y Linux. Las variantes con sabor a Linux incluyen objetivos específicos ajustados para entornos virtuales (por ejemplo, archivos VMSD y VMDK). Las cargas útiles Fog también intentarán terminar varios procesos asociados con estos entornos virtualizados.

Al realizar el cifrado, se añaden las extensiones ".fog", ".Fog" o ".FLOCKED" a los archivos afectados.

La evidencia forense indica que los actores de amenazas pudieron acceder a los entornos de las víctimas aprovechando las credenciales de VPN comprometidas. En particular, el acceso remoto se produjo a través de dos proveedores de puerta de enlace de VPN independientes.

En uno de los casos, se observó actividad de pass-the-hash contra cuentas de administrador que luego se usaron para establecer conexiones RDP a servidores Windows que ejecutaban Hyper-V y Veeam.

En las infecciones se observa que los dispositivos afectados realizan una cantidad inusual de conexiones internas fallidas a otras ubicaciones internas a través de puertos como 80 (HTTP), 3389 (RDP), 139 (NetBIOS) y 445 (SMB). Este patrón de actividad indicaba claramente un comportamiento de escaneo de reconocimiento dentro de las redes afectadas. Una investigación más a fondo de estas conexiones HTTP reveló casos comúnmente asociados con el uso de la herramienta Nmap.

Al mismo tiempo, se observó que algunos dispositivos realizaban acciones SMB dirigidas al recurso compartido IPC$. Dicha actividad se alinea con las tácticas de enumeración SMB típicas, mediante las cuales los atacantes consultan la lista de servicios que se ejecutan en un host remoto utilizando una sesión NULL, un método que se emplea a menudo para recopilar información sobre recursos de red y vulnerabilidades.

Mientras los atacantes intentan moverse lateralmente a través de las redes afectadas, se observa una actividad RDP sospechosa entre los dispositivos infectados. Se establecieron múltiples conexiones RDP con nuevos clientes, utilizando los dispositivos como pivotes para propagarse más profundamente en las redes.

Después de esto, los dispositivos en múltiples redes exhibieron un alto volumen de actividad de lectura y escritura SMB, con nombres de archivos de unidades compartidas internas con la extensión ".flocked" (o similar), una clara señal de cifrado de ransomware. Casi al mismo tiempo, se detectaron múltiples archivos "readme.txt" distribuidos en las redes afectadas, que luego se identificaron como notas de rescate.

En uno de los casos del ransomware Fog, se observó una posible exfiltración de datos que implicaba la transferencia de archivos internos a un punto final inusual asociado con el servicio de almacenamiento de archivos MEGA.

Este intento de exfiltración sugiere el uso de tácticas de doble extorsión, donde los actores de amenazas no solo cifran los datos de la víctima, sino que también los exfiltran para amenazar con exponerlos públicamente a menos que se pague un rescate. Esto a menudo aumenta la presión sobre las organizaciones, ya que enfrentan el riesgo de pérdida de datos y daño a la reputación causado por la divulgación de información confidencial.

3. RECOMENDACIONES:

- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Habilite la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados. Así como también reportar el ransomware a las autoridades.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2024/12/ransomware-fog-activo-en-america-latina.html • hxxps://darktrace.com/blog/lifting-the-fog-darktraces-investigation-into-fog-ransomware

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°280	Fecha: 04-12-2024
		Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Uso posterior a la liberación en Google Chromium		
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 uso posterior a la liberación en Google Chromium. 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-2024-4558 de tipo uso posterior a la liberación en Google Chromium, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de uso después de la liberación dentro del componente ANGLE en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, generar un error de uso después de la liberación y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de la vulnerabilidad podría permitir a un atacante comprometer el sistema vulnerable.

A. Productos afectados:

- Google Chromium: 124.0.6367.0 - 124.0.6367.154.

3. **RECOMENDACIÓN:**

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_7.html • hxxps://crbug.com/337766133 • hxxps://webkitgtk.org/security/WSA-2024-0004.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°280	Fecha: 04-12-2024 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de severidad crítica en productos Siemens		
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:

Siemens ha publicado múltiples vulnerabilidades de severidad **CRÍTICA** de tipo autenticación faltante para función crítica, desreferencia de puntero nulo, limitación incorrecta de una ruta de acceso a un directorio restringido (Path Traversal), neutralización incorrecta de elementos especiales utilizados en un comando del SO (OS Command Injection) que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado obtener acceso a la interfaz web de administración o generar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-0012 de tipo falta autenticación para función crítica en el software PAN-OS de Palo Alto Networks, podría permitir que un atacante no autenticado con acceso de red a la interfaz web de administración obtenga privilegios de administrador de PAN-OS y realice acciones administrativas, altere la configuración o explote otras vulnerabilidades de escalada de privilegios autenticados como CVE-2024-9474.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-2550 de tipo desreferencia de puntero nulo en la puerta de enlace GlobalProtect del software PAN-OS de Palo Alto Networks, podría permitir que un atacante no autenticado detenga el servicio GlobalProtect en el firewall mediante el envío de un paquete especialmente diseñado que provoca una condición de denegación de servicio. Los intentos repetidos de activar esta condición hacen que el firewall entre en modo de mantenimiento.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-2552 de tipo inyección de comandos en el software PAN-OS de Palo Alto Networks, podría permitir a un administrador autenticado eludir las restricciones del sistema en el plano de administración y eliminar archivos en el firewall.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-9474 de tipo de escalada de privilegios en el software PAN-OS de Palo Alto Networks, podría permitir que un administrador de PAN-OS con acceso a la interfaz web de administración realice acciones en el firewall con privilegios de root.

A. Productos afectados:

- RUGGEDCOM APE1808: todas las versiones (CVE-2024-2550).
- RUGGEDCOM APE1808: todas las versiones (CVE-2024-0012, CVE-2024-2552, CVE-2024-9474).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.
- Proteger el acceso a la red de los dispositivos con mecanismos adecuados. Para operar los dispositivos en un entorno de TI protegido, Siemens recomienda configurar el entorno de acuerdo con las pautas operativas de Siemens para seguridad industrial y seguir las recomendaciones de los manuales de productos.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-338-02 • hxxps://www.siemens.com/industrialsecurity • hxxps://security.paloaltonetworks.com/CVE-2024-0012 • hxxps://www.siemens.com/cert/operational-guidelines-industrial-security

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°280	Fecha: 04-12-2024 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en Service Provider Console de Veeam		
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:

Veeam ha lanzado actualizaciones de seguridad que corrigen dos vulnerabilidades de severidad **CRÍTICA** y **ALTA** que afecta a Service Provider Console (VSPC). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado la ejecución remota de código en la máquina del servidor VSPC.

2. DETALLES:

Veeam Service Provider Console es una plataforma basada en la nube que permite a las empresas gestionar y supervisar las operaciones de backup en sus oficinas. Los proveedores de servicios también la utilizan para ofrecer servicios de backup como servicio (BaaS) y recuperación ante desastres como servicio (DRaaS) a los clientes. La solución utiliza agentes de administración para interactuar con máquinas en infraestructuras administradas que ejecutan productos de respaldo, recuperación ante desastres y monitoreo/informes de TI de Veeam.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-42448, existe debido a que, desde la máquina del agente de administración de VSPC, bajo la condición de que el agente de administración esté autorizado en el servidor, es posible realizar la ejecución remota de código en la máquina del servidor de VSPC. Esto permite a los atacantes ejecutar código arbitrario de forma remota en servidores sin parches, lo que plantea graves amenazas a la integridad de los datos y la seguridad operativa. La falla afecta específicamente a los agentes de administración autorizados conectados a servidores VSPC vulnerables, lo que permite un posible control del servidor por parte de atacantes. Una explotación exitosa podría provocar acceso no autorizado, exfiltración de datos e interrupción de los procesos de respaldo y recuperación esenciales para la continuidad del negocio.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-42449 existe debido a que, desde la máquina del agente de administración de VSPC, bajo la condición de que el agente de administración esté autorizado en el servidor, es posible filtrar un hash NTLM de la cuenta de servicio del servidor VSPC y eliminar archivos en la máquina del servidor VSPC. La capacidad de obtener hashes NTLM puede provocar una escalada de privilegios dentro del sistema, lo que permite el acceso no autorizado a recursos críticos. Además, las capacidades de eliminación de archivos pueden interrumpir las operaciones y facilitar otras actividades maliciosas, como la implementación de ransomware.

A. Productos afectados:

- Veeam Service Provider Console 8.1.0.21377 y todas las versiones anteriores de las compilaciones 7 y 8.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 8.1.0.21999 que aborda esta vulnerabilidad. No existe ningún método de mitigación disponible para estas vulnerabilidades. La única solución es actualizar a la última versión de Veeam Service Provider Console.
- Limitar el acceso al servidor únicamente a agentes de administración confiables.
- Utilizar autenticación multifactor (MFA), realizar auditorías de seguridad periódicas y garantizar que todos los sistemas se mantengan actualizados.
- Utilizar versiones compatibles de Veeam Service Provider Console (versiones 7 y 8) que actualicen al último parche acumulativo. Se recomienda encarecidamente a los proveedores de servicios que utilicen versiones no compatibles que actualicen a la última versión de Veeam Service Provider Console.

Fuente de Información:	• hxxps://www.veeam.com/kb4679

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°280	Fecha: 04-12-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de omisión de verificación de imagen de software de 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 ha publicado una vulnerabilidad de severidad **ALTA** de tipo omisión de verificación de imagen de software de Cisco NX-OS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado con acceso físico a un dispositivo afectado, o un atacante local autenticado con credenciales administrativas, eludir la verificación de la firma de la imagen de NX-OS.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20397 de tipo omisión de verificación de imagen de software de Cisco NX-OS, podría permitir a un atacante no autenticado con acceso físico a un dispositivo afectado, o un atacante local autenticado con credenciales administrativas, eludir la verificación de la firma de la imagen de NX-OS.

Esta vulnerabilidad se debe a una configuración insegura del cargador de arranque. Un atacante podría aprovechar esta vulnerabilidad ejecutando una serie de comandos del cargador de arranque. Una explotación exitosa podría permitir al atacante eludir la verificación de la firma de la imagen de NX-OS y cargar software no verificado.

Cabe señalar que 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:

- CMDS 9000 Series Multilayer Switches.
- Nexus 3000 Series Switches.
- Nexus 7000 Series Switches.
- Nexus 9000 Series Fabric Switches in ACI mode.
- Nexus 9000 Series Switches in standalone NX-OS mode.
- UCS 6400 Series Fabric Interconnects.
- UCS 6500 Series Fabric Interconnects.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas. Por otro lado, Cisco no ha publicado ni publicará actualizaciones de software para los switches Cisco Nexus 92160YC-X porque este producto ha alcanzado el fin del soporte de seguridad y vulnerabilidad.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL • hxxps://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/eos-eol-notice-c51-743538.html

Índice alfabético