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

134-2025-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°134	Fecha: 10-06-2025
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Herramientas de IA falsas se utilizan para difundir malware Noodlophile		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

En plena etapa dorada de la inteligencia artificial, no es de extrañar que los cibercriminales estén adaptando sus estrategias para aprovechar el entusiasmo global de los usuarios por estas herramientas.

2. **DETALLES:**

Se han identificado campañas de ciberataques que utilizan sitios web y aplicaciones falsas de IA para distribuir ransomware o stealer, específicamente dirigidas a pequeñas empresas que buscan mejorar su productividad mediante herramientas tecnológicas, como: Nova Leads, el reconocido ChatGPT y la plataforma de video impulsada por inteligencia artificial InVideo AI.

Estas páginas imitan a empresas legítimas, ofreciendo herramientas de IA inexistentes. Cuando la víctima descarga e instala la herramienta se ejecuta el ransomware en su sistema.

Cabe indicar que, mediante técnicas de optimización de motores de búsqueda, estan logrando que los sitios maliciosos aparezcan en los primeros resultados. También se promocionan con fuerza en grupos de Facebook, campañas virales e incluso anuncios patrocinados.

Una última amenaza detectada responde al nombre de Noodlophile Stealer, un ladrón de información mediante malware que se propaga a través de plataformas falsas y editores de generación de contenido con IA, especialmente para los entusiastas del vídeo.

Se insta a los usuarios a hacer clic en enlaces que anuncian servicios de creación de contenido con IA, como vídeos, logotipos, imágenes e incluso sitios web. Uno de los sitios web falsos se hace pasar por CapCut AI y ofrece a los usuarios un editor de vídeo todo en uno con nuevas funciones de IA.

Una vez que los usuarios cargan sus imágenes o videos en estos sitios, se les pide que descarguen el supuesto contenido generado por IA, y es ahí donde se descarga en su lugar un archivo ZIP malicioso ("VideoDreamAI.zip").

Éste contiene un archivo engañoso que inicia la cadena de infección al ejecutar un binario legítimo asociado con el editor de vídeo de ByteDance ("CapCut.exe"). Este ejecutable basado en C++ se utiliza para ejecutar un cargador basado en .NET llamado CapCutLoader que, a su vez, carga una carga útil de Python ("srchost.exe") desde un servidor remoto. Finalmente, éste carga el Noodlophile Stealer, que permite recopilar credenciales del navegador, información de la billetera de criptomonedas y otros datos confidenciales.

Algunas instancias también han integrado el ladrón con un troyano de acceso remoto como XWorm para obtener acceso atrincherado a los hosts infectados.

3. **RECOMENDACIONES:**

- Asegurarse que las herramientas de IA que se descargue vengan de sitios oficiales y verificados
- Implementar un software de seguridad actualizado que pueda detectar y bloquear este tipo de amenazas.
- Mantener copias de seguridad regulares de datos importantes para minimizar el impacto.
- Capacitar a los empleados sobre los riesgos de descargar software de fuentes no confiables y sobre cómo identificar posibles amenazas.

Fuente de Información:	• hxxps://thehackernews.com/2025/05/fake-ai-tools-used-to-spread.html • hxxps://seguridad.cicese.mx/rec/2458/Parecen-editores-con-IA,-pero-esconden-malware:-evita-estas-herramientas-falsas

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°134	Fecha: 10-06-2025 Página: 5 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña de ransomware "*NightSpire*" dirigido a múltiples sectores en todo el mundo		
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:

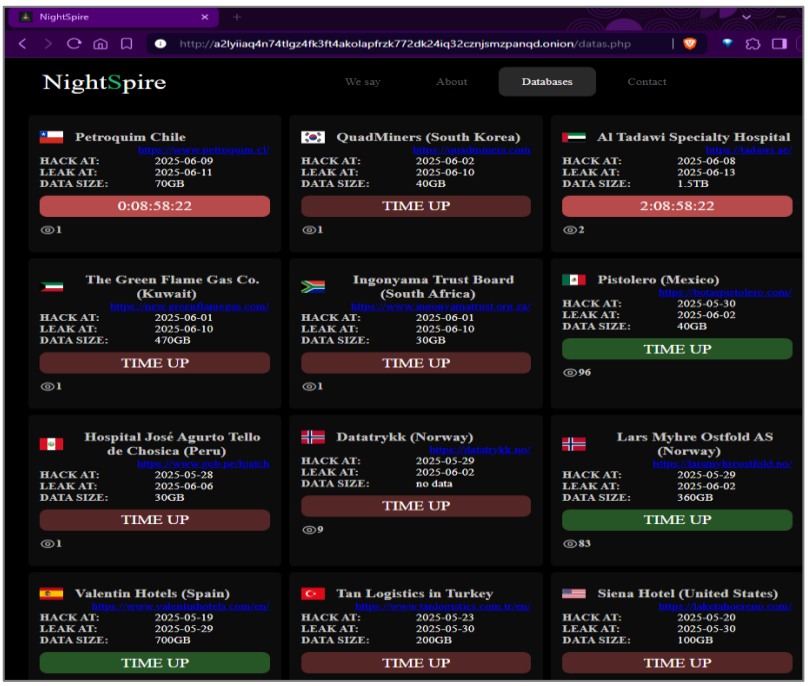
El equipo de trabajo de Seguridad Digital de la DINI ha detectado una nueva campaña de ransomware "*NightSpire*" dirigido a múltiples sectores en todo el mundo. El objetivo principal de esta campaña es obtener ganancias financieras por medio de la exfiltración y el cifrado de datos, el malware cifra los datos de sus potenciales víctimas, luego de exfiltrar la información amenaza con publicar la información en su sitio web de filtración de datos de la Dark Web si no paga el rescate, la información exfiltrada se hará de dominio público, generando un daño a la imagen de la entidad, pérdidas económicas e implicación en demandas legales y regulatorias.

2. DETALLES:

"*NightSpire*" es un grupo de ransomware con motivaciones financieras que surgió a principios de marzo del 2025 y emplea tácticas de doble extorsión. Inicialmente centrado en la exfiltración de datos y el cifrado de datos, "*NightSpire*" cifra los datos de sus potenciales víctimas, luego de exfiltrar la información amenaza con publicar la información en su sitio de filtración dedicado (DLS) de la Dark Web si no paga el rescate.

El grupo les da un plazo de tiempo a sus víctimas para que puedan negociar el rescate a través de sus canales de comunicación dejados en la nota de rescate, en caso la víctima se niegue a negociar o no pague el rescate, la información exfiltrada se hará de dominio público, generando un daño a la imagen de la entidad, pérdidas económicas e implicación en demandas legales y regulatorias.

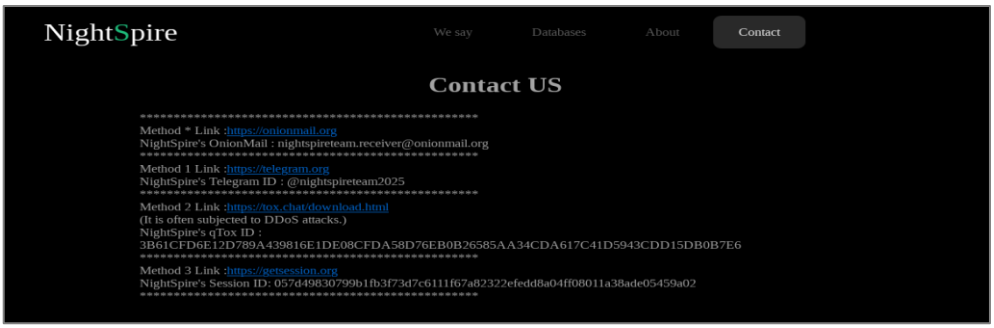
A la fecha, el grupo ya ha afectado a 57 entidades, tanto públicas como privadas en todo el mundo, países como Chile, **Perú**, Venezuela, EEUU, Canadá, Brasil, Costa Rica, Argentina se han visto comprometidos:



Fuente: hxxp://a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion/datas.php

El grupo del ransomware "*NightSpire*" utiliza principalmente tácticas de ingeniería social mediante phishing, suplantación de identidad, inducción de miedo y urgencia, y técnicas de fraude para engañar a sus víctimas y lograr que ejecuten la carga útil del malware en sus sistemas

Para sus comunicaciones, el grupo emplea plataformas encriptadas como ProtonMail, OnionMail, qTox, Telegram, getsession y portales de la Dark Web para negociar, presionar e intimidar a sus víctimas con exfiltrar la información si en caso no pagan el rescate.



Asimismo, "*NightSpire*" explota principalmente una vulnerabilidad crítica de día cero en los firewalls con sistema operativo FortiOS versión 7.0.0 a 7.0.16 y el gateway para seguridad web FortiProxy 7.0.0 a 7.0.19 y 7.2.0 a 7.2.12 de la marca Fortinet, Inc., identificada como CVE-2024-55591 de tipo omisión de autenticación mediante una ruta o canal alternativo, para obtener acceso inicial. Esta vulnerabilidad permite a los atacantes obtener acceso con el perfil de administrador "super_admin" no autorizado sin credenciales válidas, a través de solicitudes diseñadas al módulo websocket Node.js o a través de solicitudes de proxy CSF diseñadas, lo que les permite realizar cambios de configuración y acceder lateralmente a la red de la víctima.

Un ataque exitoso podría permitir a un actor de amenaza obtener privilegios de "super_admin", crear nuevas cuentas de administrador y usuarios locales con nombres aleatorios y agregarlos a los grupos de VPN SSL, modificar las políticas y configuraciones del firewall, establecer túneles VPN SSL a redes internas y obtener control total sobre el dispositivo objetivo.

"*NightSpire*" ataca aplicaciones públicas como firewalls y dispositivos VPN, para ello utiliza múltiples kits de explotación actualizados y disponibles para FortiOS como su principal punto de entrada.

Además de explotar la vulnerabilidad CVE-2024-55591, "*NightSpire*" también puede usar credenciales robadas o forzadas, incluido el acceso mediante el Protocolo de Escritorio Remoto (RDP), para obtener acceso inicial. Sus tácticas de acceso inicial se alinean con la técnica MITRE ATT&CK T1190 (Explotar aplicación pública).

"*NightSpire*" representa una amenaza nueva de ransomware que combina el cifrado tradicional con el robo de datos y el daño a la reputación para maximizar el impacto de la extorsión. El uso de exploits de tipo día cero, tácticas de explotación agrícola y canales de comunicación cifrados son un riesgo de alta criticidad para organizaciones con prácticas de ciberseguridad deficientes.

El modelo de doble extorsión del grupo y su objetivo global en sus ciberataques requieren que se implementen estrategias de seguridad, que implica desarrollar y aplicar medidas para proteger los activos digitales de la entidad.

En el Perú, las entidades públicas y privadas que cuenten con equipos vulnerables de la marca Fortinet podrían estar expuestos a estos tipos de ciberataques de ransomware. Un atacante podría obtener privilegios de "super_admin", crear nuevas cuentas de usuarios locales y de administrador, con nombres aleatorios y agregarlos a los grupos de SSL VPN, modificar las políticas y configuraciones del firewall, establecer túneles VPN SSL a redes internas y obtener control total sobre el dispositivo objetivo, así como la exfiltración y cifrados de los activos digitales que han sido comprometidos.

Los responsables de Tecnologías de la Información y la Comunicación, administradores de red, servidores y el área de seguridad de la información de las instituciones y entidades públicas o privadas, deben *monitorear permanentemente* las nuevas vulnerabilidades, amenazas y eventos inusuales que podrían afectar los activos digitales.

A. Indicadores de compromiso (IoC):

Entradas de registros:

- Registro de actividad de inicio de sesión con scripts y dstip (dirección IP de destino) aleatorios:

  type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1733486785" user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin logged in successfully from jsconsole".

- Registro de creación de administrador con nombre de usuario y dirección IP de origen generados aleatoriamente:

  type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="admin" ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin" cfgobj="vOcep" cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin vOcep".

- Direcciones IP utilizadas por los atacantes en los registros anteriores: 1.1.1.1, 127.0.0.1, 2.2.2.2, 8.8.8.8, 8.8.4.4, 13.37.13.37.

Fortinet indicó en un informe (https://fortiguard.fortinet.com/psirt/FG-IR-24-535), que se debe tener en cuenta que los parámetros IP anteriores no son las direcciones IP de origen reales del tráfico de ataque, sino que son generados aleatoriamente por el atacante como parámetro del ataque. Por lo tanto, no deben utilizarse para ningún bloqueo.

Fortinet indico que, de acuerdo a los análisis realizados, se pudo observar las siguientes actividades maliciosas realizadas por el actor de amenaza:

- Crear una cuenta de administrador en el dispositivo con un nombre de usuario aleatorio.
- Crear una cuenta de usuario local en el dispositivo con un nombre de usuario aleatorio.
- Crear un grupo de usuarios o agregar el usuario local anterior a un grupo de usuarios sslvpn existente.
- Agregar/cambiar otras configuraciones (política de firewall, dirección de firewall, etc).
- Iniciar sesión en una VPN con capa de sockets seguros (SSL VPN) con los usuarios locales agregados anteriormente para obtener un túnel a la red interna.

El usuario “Admin” o “Local” creado por el actor de amenaza se generó aleatoriamente y utilizó las siguientes direcciones IP:

- 45.55.158.47 [dirección IP más utilizada].
- 87.249.138.47.
- 155.133.4.175.
- 37.19.196.65.
- 149.22.94.37.
- 158.255.215.126.

Hashes:

- MD5: 0170601e27117e9639851a969240b959.
- SHA1: 7a4aee1910b84c6715c465277229740dfc73fa39.
- SHA256: 35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7.
- Dominio en Dark Web: a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion.

3. RECOMENDACIONES:

- Realizar copias de seguridad permanente de la información crítica en dispositivos externos desconectados o en la nube, deben estar aisladas del sistema principal para evitar que el ransomware los afecte. Verificar regularmente la integridad y restaurabilidad de estas copias.
- Mantener actualizado el sistema operativo, aplicaciones y todos los programas instalados en los dispositivos.
- Utilizar un software antimalware/antivirus con protección en tiempo real y funciones específicas contra ransomware.
- Configurar el cortafuego y limitar los servicios expuestos, como el Protocolo de Escritorio Remoto (RDP), que suelen ser utilizados como vectores de ciberataques.
- No abrir archivos adjuntos ni hacer clic en enlaces de correos electrónicos sospechosos o de remitentes desconocidos, ya que los ataques de phishing es uno de los métodos principales de distribución de ransomware "*NightSpire*".
- Descargar software solo de fuentes oficiales y evitar programas piratas o cracks.
- Desactivar la ejecución automática de macros en documentos de Office, ya que suelen ser usados para distribuir ransomware.
- Utilizar cuentas sin privilegios de administrador para las tareas diarias y limitar el acceso a recursos críticos.
- Segmentar la red para que un posible ataque no se propague fácilmente a otros sistemas.
- Implementar la autenticación multifactor (MFA) para acceder a sistemas y copias de seguridad.
- Concientizar a los usuarios para que reconozcan intentos de ataques de phishing y apliquen las buenas prácticas de seguridad digital.

Fuente de Información:	• Equipo de trabajo de Seguridad Digital DINI.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°134	Fecha: 10-06-2025
		Página: 9 de 12

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

Wazuh Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo deserialización de datos no confiables que afecta a la plataforma de ciberseguridad de código abierto Wazuh. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado la ejecución remota de código en servidores Wazuh.

2. DETALLES:

Wazuh es una plataforma de seguridad gratuita y de código abierto que unifica la protección XDR (Extended Detection and Response) y SIEM (Security Information and Event Management) para endpoints y cargas de trabajo en la nube. Está diseñada para la prevención, detección y respuesta a amenazas en infraestructuras locales, nubes públicas y privadas, y centros de datos.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24016 de tipo deserialización de datos no confiables que afecta Wazuh, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

Esta vulnerabilidad está siendo explotada activamente en la naturaleza. Existen múltiples pruebas de concepto de exploits disponibles en github.com.

La vulnerabilidad existe debido a una validación de entrada insegura al procesar datos serializados en framework/wazuh/core/cluster/common.py. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Wazuh: 4.4.0 - 4.9.0.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°134	Fecha: 10-06-2025 Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el servicio de enrutamiento y acceso remoto RRAS de Microsoft		
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:

Microsoft Corporation ha publicado dos vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer basado en montón que afecta al Servicio de enrutamiento y acceso remoto (RRAS). La explotación exitosa de estas vulnerabilidades 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-2025-33066 de tipo desbordamiento de búfer basado en montón en el RRAS, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite en el RRAS. Un atacante remoto puede engañar a una víctima para que se conecte a un servidor malicioso, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-33064 de tipo desbordamiento de búfer basado en montón en el RRAS, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite en el RRAS. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema objetivo.

La explotación exitosa de estas vulnerabilidades podría resultar en el compromiso completo del sistema vulnerable.

A. Productos afectados:

- Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.4264.
- Windows Server: 2008 6.0.6003.22567 - 2025 10.0.26100.4264.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-33066 • hxxps://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-33064

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°134	Fecha: 10-06-2025
		Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica zero-day en FortiOS y FortiProxy de Fortinet		
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:

Fortinet, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de día cero de tipo omisión de autenticación mediante una ruta o canal alternativo que afecta al sistema operativo FortiOS y el gateway para seguridad web FortiProxy. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener privilegios de super_admin a través de solicitudes de proxy CSF diseñadas.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24472 de tipo omisión de autenticación mediante una ruta o canal alternativo que afecta a FortiOS y FortiProxy, podría permitir a un atacante remoto no autenticado obtener privilegios de super_admin en el sistema. Esto se logra mediante solicitudes especialmente manipuladas en el módulo de proxy CSF o en el módulo WebSocket de Node.js

Investigadores han detectado explotación activa, donde atacantes crean cuentas administrativas no autorizadas, acceden a VPN de SSL y modifican las configuraciones del firewall para acceder a redes internas.

Se ha publicado un exploit de prueba de concepto (PoC) en varios canales, lo que facilita que otros atacantes repliquen el ataque, el exploit aprovecha directamente la falla para tomar control administrativo sin necesidad de credenciales válidas.

A. Productos afectados:

- FortiVoice 7.2.1+, 7.0.7+ o 6.4.11+.
- FortiMail 7.6.3+, 7.4.5+, 7.2.8+ o 7.0.9+.
- FortiNDR 7.6.1+, 7.4.8+, 7.2.5+ o 7.0.7+.
- FortiRecorder 7.2.4+, 7.0.6+ o 6.4.6+.
- FortiCamera 2.1.4+.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Se ha lanzado un parche: actualizar a FortiOS 7.0.17 o superior, y FortiProxy 7.0.20 o 7.2.13 en adelante.
- Deshabilitar el acceso HTTP/HTTPS a la interfaz de administración del firewall o limitar el acceso por IP mediante políticas locales (“local-in”).
- Monitorear actividad sospechosa, verificar la creación de cuentas no autorizadas, cambios en políticas de firewall, conexiones inusuales en SSL VPN.
- Fortalecer accesos administrativos, se debe limitar IPs permitidas, usar autenticación multifactor y evitar exposición directa a Internet.

Fuente de Información:	• hxxps://fortiguard.fortinet.com/psirt/FG-IR-24-535

Índice alfabético