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

049-2025-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°049	Fecha: 27-02-2025
		Página: 4 de 15

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El nuevo malware de Linux “Auto-Color” otorga acceso remoto completo		
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:

Un malware para Linux descubierto recientemente, llamado Auto-Color, está atacando activamente a universidades y organizaciones gubernamentales en América del Norte y Asia

Identificado por primera vez por Unit 42 de Palo Alto Networks, Auto-Color proporciona a los atacantes acceso remoto persistente, lo que dificulta su detección y eliminación.

2. DETALLES:

Auto-Color es una pieza de malware potente y curiosa al mismo tiempo, ya que permite al atacante crear un shell inverso, ejecutar comandos para recopilar información del sistema, crear y modificar archivos, ejecutar aplicaciones, convertir el dispositivo en un proxy y hasta desinstalar el propio malware, el cual evita su detección de varias formas: usando nombres de archivo simples, ocultando sus conexiones.

Auto-color recibe su nombre en función del nombre del archivo que cambia de nombre después de la instalación de la carga inicial. Actualmente no se sabe cómo llega a sus objetivos, pero lo que sí se sabe es que requiere que la víctima lo ejecute explícitamente en su máquina Linux.

Un aspecto destacable del malware es el arsenal de métodos que emplea para evadir la detección como:

- Uso de nombres de archivos de apariencia inofensiva para operar, como "door" o "egg".
- Ocultamiento de conexiones de comando y control remoto (C2) mediante una técnica avanzada similar a la utilizada por la familia de malware Symbiote.
- Implementación de algoritmos de cifrado de tipo propietario para ocultar información de comunicación y configuración.

Una vez lanzado con privilegios de root, procede a instalar un implante de biblioteca malicioso llamado "libcext.so.2", se copia y cambia de nombre a /var/log/cross/auto-color y realiza modificaciones en "/etc/ld.preload" para establecer persistencia en el host.

Si el usuario actual no tiene privilegios de root, el malware no procederá a instalar la biblioteca evasiva en el sistema. Procederá a hacer todo lo posible en sus fases posteriores sin esta biblioteca limitando su funcionalidad.

Cuando se instala el implante malicioso de biblioteca, el contenido real de la biblioteca se encuentra dentro de la memoria del ejecutable original, específicamente en la sección .rodata.

Esta biblioteca tiene dos objetivos principales, la evasión y la persistencia:

- Ocultar la actividad de la red entre el malware y el objetivo remoto configurado dentro de una carga útil global.
- Prevención de la desinstalación mediante la protección de /etc/ld.preload contra modificaciones o eliminaciones.

El código malicioso de la biblioteca intercepta ciertas funciones de la libc para modificar la llamada al sistema open(), lo que le permite ocultar las comunicaciones con el C2 manipulando el archivo «/proc/net/tcp», que almacena información sobre las conexiones de red activas. Esta táctica ya había sido utilizada por otro malware para Linux, conocido como Symbiote.

Auto-Color, al conectarse a un servidor C2 remoto, permite a los atacantes:

- Abra un shell inverso, permitiendo a los operadores acceso remoto completo.
- Ejecutar comandos arbitrarios en el sistema.
- Modificar o crear archivos para expandir la infección.
- Actúa como un proxy, reenviando el tráfico del atacante.
- Modificar su configuración dinámicamente.

La Unidad 42 dice que Auto-Color también cuenta con un "interruptor de seguridad" incorporado, que permite a los atacantes eliminar inmediatamente los rastros de infección de las máquinas comprometidas para impedir las investigaciones.

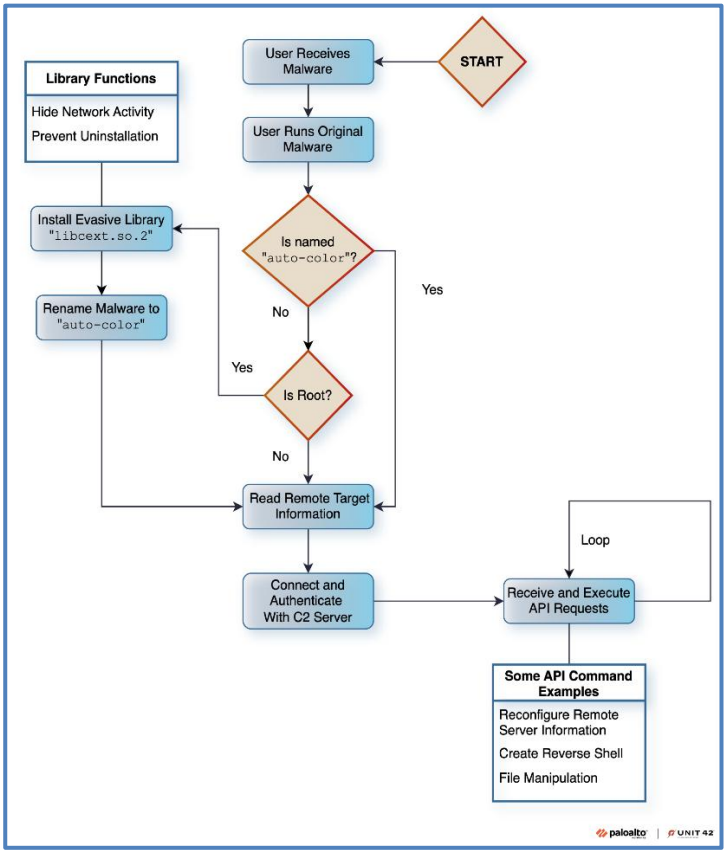


Diagrama de flujo del Auto-Color

Indicadores de Compromiso:

Archivos maliciosos de Auto-Color:

- Hash SHA256: 270fc72074c697ba5921f7b61a6128b968ca6ccbf8906645e796cfc3072d4c43
  Nombre del archivo: log
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 1 de malware de Auto-color
- Hash SHA256: 65a84f6a9b4ccddcdae812ab8783938e3f4c12cfba670131b1a80395710c6fb4
  Nombre del archivo: edus
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 2 de malware de Auto-color
- Hash SHA256: 83d50fcf97b0c1ec3de25b11684ca8db6f159c212f7ff50c92083ec5fbd3a633
  Nombre del archivo: egg
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 3 de malware de Auto-color

- Hash SHA256: a1b09720edcab4d396a53ec568fe6f4ab2851ad00c954255bf1a0c04a9d53d0a
  Nombre del archivo: edu
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 4 de malware de Auto-color

- Hash SHA256: bace40f886aac1bab03bf26f2f463ac418616bacc956ed97045b7c3072f02d6b
  Nombre del archivo: door
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 5 de malware de Auto-color

- Hash SHA256: e1c86a578e8d0b272e2df2d6dd9033c842c7ab5b09cda72c588e0410dc3048f7
  Nombre del archivo: exup
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 6 de malware de Auto-color

- Hash SHA256: 85a77f08fd66aeabc887cb7d4eb8362259afa9c3699a70e3b81efac9042bb255
  Nombre del archivo: law
  Tipo de archivo: ejecutable pie ELF LSB de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Muestra 7 de malware de Auto-color

- Hash SHA256: bf503b5eb456f74187a17bb8c08bccc9b3d91a7f0f6fd50110540b051510d1ca
  Nombre del archivo: libcext.so.2
  Tipo de archivo: objeto compartido LSB ELF de 64 bits, x86-64, versión 1 (SYSV), vinculado dinámicamente
  Descripción del archivo: Implante de biblioteca de Auto-color

Direcciones IP C2 maliciosas de Auto-Color:

- 146[.]70[.]41[.]178:443 - muestra de log
- 216[.]245[.]184[.]214:443 - muestra de edus/egg
- 146[.]70[.]87[.]67:443 - muestra de edu/door
- 65[.]38[.]121[.]64:443 - muestra exup
- 206[.]189[.]149[.]191:443 - muestra de law

Auto-Color es una clara señal de que las amenazas para Linux se están volviendo más sofisticadas y específicas. A diferencia de las botnets genéricas o el ransomware automatizado, este malware está diseñado para ser discreto, persistente y tener control a largo plazo. Su capacidad para modificar los procesos del sistema y evadir las herramientas de seguridad tradicionales lo convierte en un serio desafío para los defensores.

3. RECOMENDACIONES:

- Monitorear los cambios en '/etc/ld.preload', que es un mecanismo de persistencia clave.
- Verificar '/proc/net/tcp' para detectar anomalías de salida.
- Usar soluciones de detección de amenazas basadas en el comportamiento, como el Cortex XDR y XSIAM, los cuales bloquean y alertan sobre comportamientos e indicadores conocidos asociados con el Auto-Color.
- Inspeccionar los registros del sistema y el tráfico de red en busca de conexiones a las IP C2 enumeradas en la lista de Indicadores de Compromiso.
- Usar el filtrado de URL avanzado y la seguridad de DNS avanzada para identificar las URL y los dominios conocidos asociados con esta actividad como maliciosos.

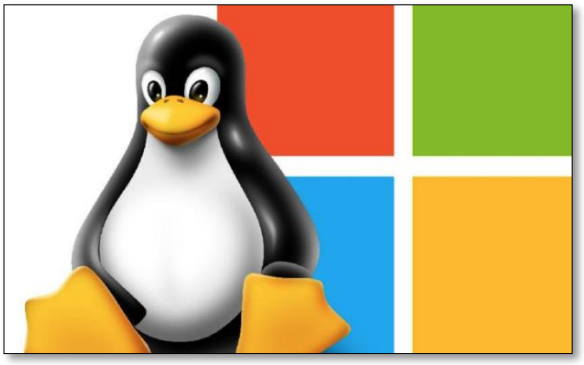
Fuente de Información:	• hxxps://unit42.paloaltonetworks.com/new-linux-backdoor-auto-color/ • hxxps://www.muylinux.com/2025/02/26/auto-color-malware/ • hxxps://thehackernews.com/2025/02/new-linux-malware-auto-color-grants.html • hxxps://www.bleepingcomputer.com/news/security/new-auto-color-linux-backdoor-targets-north-american-govts-universities/ • hxxps://zendata.security/2025/02/27/new-linux-malware-auto-color-grants-full-remote-access/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025
		Página: 7 de 15

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El nuevo ransomware Anubis ataca entornos Windows, Linux, NAS y ESXi x64/x32		
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:



Un nuevo grupo de ransomware, denominado Anubis, ha surgido como una amenaza importante en el panorama de la ciberseguridad. Activo desde finales de 2024, Anubis emplea técnicas avanzadas y opera en múltiples plataformas, incluidos entornos Windows, Linux, NAS y ESXi. El grupo está aprovechando el ransomware como servicio (RaaS) y otros modelos de monetización basados en afiliados para expandir su alcance e impacto.

2. DETALLES:

Según se informa, el ransomware Anubis se desarrolló utilizando el algoritmo de cifrado ChaCha+ECIES, lo que permite un cifrado de datos robusto. Está dirigido a arquitecturas x64/x32 en varios entornos al tiempo que eleva los privilegios a NT AUTHORITY\SYSTEM para un acceso más profundo al sistema. El malware también cuenta con capacidades de auto propagación, lo que le permite cifrar dominios enteros de manera eficiente. Estas funcionalidades se gestionan a través de un panel web fácil de usar y diseñado para afiliados. Las operaciones del grupo destacan un enfoque en industrias críticas, incluidos los sectores de salud e ingeniería. Entre sus víctimas recientes se incluyen organizaciones de Australia, Canadá, Perú y Estados Unidos. Cabe destacar que dos de sus cuatro víctimas confirmadas pertenecen al sector de la salud, lo que subraya su posible enfoque en industrias con datos confidenciales

Programas de afiliados: modelos de monetización diversificados

Anubis ha introducido una serie de programas de afiliados para atraer colaboradores cibercriminales:

A. **Ransomware como servicio (RaaS):** Los afiliados reciben el 80% de los pagos de rescate por implementar el ransomware Anubis.

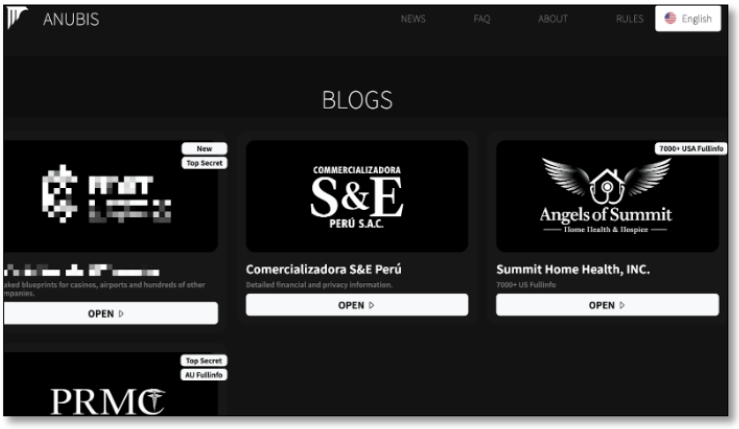
B. **Programa de rescate de datos:** Este modelo se centra en monetizar los datos robados mediante amenazas de exposición pública, ofreciendo a los afiliados el 60 % de los ingresos. Los datos robados deben cumplir criterios específicos, como exclusividad y relevancia.

C. **Programa de monetización de acceso:** Los corredores de acceso inicial pueden vender credenciales corporativas a Anubis por una participación del 50 % en los ingresos. Este programa incluye un perfil detallado de las víctimas para maximizar el poder de extorsión.

Estos programas reflejan un modelo de negocio bien estructurado orientado a maximizar la rentabilidad a través de múltiples flujos de ingresos.

Según Kela, Anubis opera con un alto grado de sofisticación.

Sus tácticas incluyen la publicación de artículos de investigación sobre las víctimas en páginas de blogs ocultas para presionar a las organizaciones a pagar rescates.



Captura de pantalla de la página de inicio del blog de Anubis

La primera víctima declarada fue el Centro Médico Pound Road (PRMC), una empresa de atención médica australiana. PRMC emitió un comunicado en el que afirmaba que había sufrido un "incidente cibernético" el 13 de noviembre de 2024 y que "un tercero no autorizado podría haber accedido y tomado los datos de los pacientes".

"Sin embargo, no se mencionó ningún ransomware, lo que sugiere que las operaciones actuales de Anubis pueden centrarse en la extorsión de datos, o lo que el propio Anubis llama 'Data Ransom', en lugar del ransomware tradicional que implica el cifrado de archivos", dijo Kela a SecurityWeek.

La investigación de Kela sugiere que hay un nuevo chico en el barrio. También sugiere que la extorsión basada únicamente en la exfiltración de datos (es decir, sin tomarse la molestia de cifrar los archivos de las víctimas) es una práctica en aumento, y que Anubis está aprovechándose de esto para ofrecer un servicio de extorsión posterior a la exfiltración.

Esto no significa que Anubis esté abandonando el modelo tradicional de cifrado RaaS. La publicación de superSonic del 23 de febrero proporciona una lista de las capacidades de cifrado del ransomware. Kela no ha tenido la oportunidad de analizar ningún código real detectado (es demasiado nuevo), por lo que no puede verificar si las afirmaciones son válidas. Pero si son ciertas, "los operadores de Anubis pueden ser personas con experiencia, posiblemente ex afiliados de otros grupos de ransomware", afirma.

Es muy pronto para que surja un nuevo grupo de amenazas, pero el profesionalismo y la experiencia demostrados en tan solo un par de meses indican que Anubis y sus afiliados podrían convertirse en una amenaza importante para las organizaciones en el transcurso de 2025.

3. RECOMENDACIONES:

- 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.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Invertir en soluciones de seguridad, como sistemas de detección y respuesta de endpoints (EDR).
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://gbhackers.com/new-anubis-ransomware-targets-windows-linux-nas-and-esxi/ • hxxps://www.fortinet.com/lat/resources/cyberglossary/ransomware-as-a-service-raas

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025 Página: 9 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el complemento ThemeMakers PayPal Express para WordPress		
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:

Wordfence ha publicado una vulnerabilidad de severidad **MEDIA** de tipo secuencias de comandos entre sitios almacenadas que afectan al complemento ThemeMakers PayPal Express Checkout para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado con permisos de colaborador o superior inyectar secuencias de comandos web arbitrarias en las páginas.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-1689 de secuencias de comandos entre sitios almacenadas que afectan al complemento ThemeMakers PayPal Express Checkout para WordPress, podría permitir a un atacante autenticado con permisos de colaborador o superior inyectar secuencias de comandos web arbitrarias en las páginas. Estas secuencias de comandos se ejecutan cuando los usuarios acceden a las páginas inyectadas.

El complemento PayPal Express Checkout de ThemeMakers para WordPress es vulnerable a secuencias de comandos entre sitios almacenados a través del código corto "PayPal" en versiones hasta la 1.1.9, debido a una limpieza de entrada insuficiente y a un escape de salida en los atributos proporcionados por el usuario.

A. Productos afectados:

- ThemeMakers PayPal Express, versión hasta la 1.1.9.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Asegurarse de que solo personas de confianza tengan permisos de nivel de colaborador o superiores en sus sitios de WordPress.

Fuente de Información:	• hxxps[:]//www[.]Wordfence[.]com/threat-intel/vulnerabilities/wordpress-plugins/tmm_paypal_checkout/thememakers-paypal-express-checkout-119-authenticated-contributor-stored-cross-site-scripting-via-shortcode • hxxps[:]//github[.]com/ThemeMakers/tmm_paypal_checkout/commit/d6d3b1877ed705ac171cf7e74a6e866fc135ba22

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025
		Página: 10 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el sistema de gestión de red Netgear ProSAFE Network Management System		
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:

Netgear, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo ejecución remota de código (RCE) que afecta al sistema de gestión de red Netgear ProSAFE Network Management System (NMS300). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en los sistemas afectados, siempre que tengan credenciales de autenticación.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-5246 de tipo ejecución remota de código que afecta al sistema de gestión de red Netgear ProSAFE NMS300, podría permitir a un atacante remoto ejecutar código arbitrario en los sistemas afectados, siempre que tengan credenciales de autenticación.

Esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas del sistema de gestión de red NETGEAR ProSAFE. La falla existe en el instalador del producto, el problema es el resultado del uso de una versión vulnerable de Apache Tomcat. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de SYSTEM.

A. Productos afectados:

- ProSAFE NMS300, versiones anteriores a 1.7.0.37.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar los sistemas para protegerse contra posibles ataques de inyección SQL.
- Actualizar Apache Tomcat a una versión parcheada, asegure el acceso a interfaces sensibles y revise periódicamente las configuraciones.

Fuente de Información:	• hxxps://kb.netgear.com/000066164/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2024-0003-PSV-2024-0004

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025 Página: 11 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en la cámara Trivision NC227WF de TrivisionSecurity		
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 dos vulnerabilidades de severidad **ALTA** de tipo transmisión de contraseñas y omisión de autenticación que afectan a la cámara Trivision NC227WF de TrivisionSecurity. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante recuperar credenciales de administrador en texto sin formato mediante el envío de una solicitud al servidor, lo que podría exponer información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1738 de tipo transmisión de contraseña a través de cadenas de consulta que afectan a la cámara Trivision NC227WF, podría permitir a un atacante recuperar credenciales del administrador sin autenticación adecuada. Esta vulnerabilidad expone información confidencial al transmitir contraseñas en texto plano a través de la cadena de consulta de una URL, lo que permite a terceros acceder a esta información sensible;

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1739 de tipo omisión de autenticación que afectan a la cámara Trivision NC227WF, podría permitir a un atacante recuperar credenciales de administrador sin autenticación adecuada. Esta se logra enviando una solicitud contra el servidor utilizando herramientas como "curl" con credenciales aleatorias a una URL específica, como "/es/player/activex_pal.asp", lo que da como resultado una autenticación exitosa sin una validación adecuada.

A. Productos afectados:

- Cámara Trivision NC227WF, versión 5.8.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps[:]//www[.]incibe[.]es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-trivision-camera-nc227wf • hxxps[:]//trivisionsecurity[.]com/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025 Página: 12 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en complementos para WordPress		
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:

Wordfence ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo gestión inadecuada de privilegios, omisión de autenticación mediante una ruta o canal alternativo y Cross-site Scripting que afectan a varios complementos para WordPress. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado escalar privilegios, iniciar sesión como administrador e inyectar secuencias de comandos web arbitrarias en páginas que se ejecutarán siempre que un usuario acceda a una página inyectada.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1295 de tipo gestión inadecuada de privilegios en el complemento Templines Elementor Helper Core para WordPress, podría permitir a los atacantes autenticados con acceso de nivel de suscriptor o superior actualizar su Wordfence s metadatos de usuario y escalar sus privilegios a administrador. Esto solo se puede explotar cuando el complemento BuddyPress también está instalado y activado. Un atacante podría obtener acceso administrativo completo a un sitio de WordPress, comprometer por completo la seguridad del sitio web y modificar la configuración del sitio, el contenido y las cuentas de usuario e instalar complementos o temas maliciosos, así como acceder a datos confidenciales del sitio y del usuario.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1717 de tipo omisión de autenticación en el complemento Login Me Now para WordPress, se origina en un mecanismo de autenticación inseguro en la función 'AutoLogin::listen()', que permite a atacantes no autenticados iniciar sesión como usuarios existentes, incluidos potencialmente administradores. Un atacante podría obtener acceso no autorizado a sitios de WordPress que ejecuten versiones vulnerables del complemento Login Me Now. Esto podría dar lugar a la apropiación total del sitio, el robo de datos, la manipulación de contenido o el uso del sitio comprometido para otras actividades maliciosas. La capacidad de iniciar sesión como administrador presenta un riesgo crítico de seguridad.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-6261 en el complemento Image Photo Gallery Final Tiles Grid para WordPress, es vulnerable a un ataque de secuencias de comandos entre sitios almacenados a través del código abreviado 'FinalTilesGallery' del complemento, debido a una limpieza de entrada insuficiente y al escape de salida en los atributos proporcionados por el usuario. Esto hace posible que atacantes autenticados, con acceso de nivel de colaborador y superior, inyecten secuencias de comandos web arbitrarias en páginas que se ejecutarán siempre que un usuario acceda a una página inyectada.

Wordfence indico que no hay evidencia de que exista una prueba de concepto pública.

A. Productos afectados:

- Complemento Templines Elementor Helper Core, versiones hasta la 2.7 inclusive.
- Complemento Login Me Now, versiones hasta la 1.7.2 inclusive.
- Complemento Image Photo Gallery Final Tiles Grid, versiones hasta la 3.6.0 inclusive.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.wordfence.com/threat-intel/vulnerabilities/id/8c5aa062-b9a2-4ddb-a5bf-4c8368218e85?source=cve • hxxps://www.wordfence.com/threat-intel/vulnerabilities/id/fc689622-50d6-47c4-a5f6-0314b1a207c9?source=cve • hxxps://www.wordfence.com/threat-intel/vulnerabilities/id/8d945c4b-3eb1-4bab-b355-117b7fd06553?source=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025 Página: 13 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en la condición de carrera de configuración de sesión ksmbd del kernel de Linux		
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 **CRÍTICA** de tipo condición de carrera que afecta al kernel de Linux. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en las instalaciones afectadas del kernel de Linux.

2. DETALLES:

ksmbd es un servidor SMB3 implementado en el kernel de Linux, diseñado para mejorar el rendimiento en comparación con soluciones tradicionales como Samba.

La vulnerabilidad de severidad **crítica** de tipo configuración de sesión ksmbd del kernel de Linux, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en las instalaciones afectadas del kernel de Linux. No se requiere autenticación para explotar esta vulnerabilidad. Sin embargo, solo los sistemas con ksmbd habilitado son vulnerables.

La falla específica existe en la implementación de la configuración de la sesión. El problema surge de la falta de un bloqueo adecuado al realizar operaciones en un objeto. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del núcleo.

Esta vulnerabilidad está programada para su divulgación pública el 1 de abril de 2025. Sin embargo, los detalles específicos sobre la naturaleza de la vulnerabilidad, como si implica una escalada de privilegios u otros tipos de exploits, aún no están disponibles públicamente.

A. Productos afectados:

- Kernel de Linux, múltiples versiones.

3. RECOMENDACIONES:

- Actualizar el kernel de Linux a la última versión disponible que aborda esta vulnerabilidad.
- Implementar la autenticación multifactor (MFA), agregará una capa adicional de seguridad, lo que dificulta que los atacantes obtengan acceso no autorizado.
- Limitar los privilegios del usuario para reducir el impacto potencial de una vulnerabilidad.
- Emplear sistemas de detección y prevención de intrusiones, firewalls y software antimalware para monitorear actividades sospechosas.
- Segmentar la red para limitar el movimiento lateral en caso de una vulnerabilidad.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-25-100/ • hxxps://web.git.kernel.org/pub/scm/linux/kernel/git/stable/stable-queue.git/commit/?id=0a1483d5bf25bcd0974db5ac284d575be6f4e47f

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°049	Fecha: 27-02-2025 Página: 14 de 15

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el software CNCSoft-G2 DPAX de Delta Electronics		
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 desbordamiento de búfer basado en pila en el análisis de archivos del software de interfaz hombre-máquina (HMI) CNCSoft-G2 DPAX de Delta Electronics. 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-2025-22880 de tipo desbordamiento de búfer basado en pila en el análisis de archivos CNCSoft-G2 DPAX de Delta Electronics, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino. Para explotar esta vulnerabilidad es necesaria la interacción del usuario, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso.

La falla específica existe en el análisis de archivos DPAX. El problema surge de la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos a un búfer basado en montón de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

A. Productos afectados:

- CNCSoft-G2: versiones anteriores a la 2.1.0.20.

3. RECOMENDACIONES:

- Actualizar a la versión v2.1.0.20 o posterior que aborda esta vulnerabilidad.
- Implementar actualizaciones de software periódicas para todo el software, no solo para CNCSoft-G2.
- Restringir el acceso de los usuarios a los sistemas que utilizan CNCSoft-G2.
- No hacer clic en enlaces de Internet que no sean confiables ni abra archivos adjuntos no solicitados en correos electrónicos.
- Evitar exponer los sistemas y equipos de control a Internet.
- Colocar los sistemas y dispositivos detrás de un firewall y aíslelos de la red empresarial.
- Utilizar un método de acceso seguro, como una red privada virtual (VPN), cuando se requiera acceso remoto.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-25-098/ • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

Índice alfabético