Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

HACKERS USAN UN FALLO EN WINRAR PARA INFECTAR COMPUTADORAS CON MALWARE

18/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente investigadores encontraron una vulnerabilidad zero-day en WinRAR, registrada como CVE-2025-8088, los investigadores encontraron que está siendo explotada activamente en ataques dirigidos por el grupo RomCom, también conocido como Strom-0978, UNC2596, Tropical Scorpius.

HACKERS USAN UN FALLO EN WINRAR PARA INFECTAR COMPUTADORAS CON MALWARE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	18/08/2025
Es día cero (0 day):	Si

RESUMEN

Recientemente investigadores encontraron una vulnerabilidad zero-day en WinRAR, registrada como CVE-2025-8088, los investigadores encontraron que está siendo explotada activamente en ataques dirigidos por el grupo RomCom, también conocido como Strom-0978, UNC2596, Tropical Scorpius.

La falla es de tipo path traversal, está permite que archivos dentro de un archivo RAR maliciosamente configurado se extraigan fuera de la carpeta elegida por el usuario, incluso en rutas sensibles como las de arranque automático (Startup) de Windows.

¿Cómo funciona?

- El atacante envía un archivo .rar disfrazado de CV, documento oficial u otro archivo convincente.
- Al extraerlo con WinRAR (versiones anteriores a la 7.13), el exploit fuerza la extracción de un archivo malicioso directamente en una ruta como %APPDATA%\…\Startup, que se ejecuta automáticamente al iniciar sesión en Windows.
- Este archivo actúa como instalador de malware, lo que permite ejecución remota de código al siguiente inicio del sistema.

Versiones afectadas

Afecta a las versiones anteriores a las 6.23, esto quiere decir que todas las ramas 6.22 y anteriores son vulnerables.

La versión 6.23 lanzada por RARLAB ya incluye el parche de seguridad que corrige esta falla.

Cabe recalcar que WinRAR no contiene una función de actualización automática, por lo que los usuarios deben descargar e instalar manualmente la última versión.

RECOMENDACIONES

- nstalar la versión 6.23 o superior, que corrige la vulnerabilidad.
- Descargar siempre desde el sitio oficial de RARLAB para evitar versiones manipuladas.
- No abrir .RAR o .ZIP recibidos por correo, mensajería o foros si no se confía en la fuente.
- Prestar atención especial a archivos relacionados con trading, inversiones o criptomonedas, ya que fueron usados en campañas activas.
- Tratar cualquier archivo externo como potencialmente malicioso hasta verificar su procedencia.

NOTICIA COMPLETA

https://devel.group/blog/hackers-usan-un-fallo-en-winrar-para-infectar-computadoras-con-malware/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group