Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°195	Fecha: 20-08-2023
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad 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 descubierto una vulnerabilidad crítica en WinRAR, la popular utilidad de archivado de archivos para Windows. Identificada como CVE-2023-40477, ha generado preocupación debido a su gravedad y al potencial que tiene para permitir a los atacantes ejecutar comandos en una computadora simplemente al abrir un archivo RAR.

El investigador "goodbyeselene" de Zero Day Initiative fue quien descubrió esta falla en el procesamiento de los volúmenes de recuperación de WinRAR.

2. DETALLES:

La vulnerabilidad radica en la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede conducir a un acceso no autorizado a la memoria más allá del final de un búfer asignado.

Esta debilidad podría ser explotada por atacantes remotos para ejecutar código arbitrario en el sistema de destino.

"La falla específica existe en el procesamiento de los volúmenes de recuperación", se lee en el aviso de seguridad publicado en el sitio de ZDI.

"El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en un acceso a la memoria más allá del final de un búfer asignado".

Como un objetivo necesita engañar a una víctima para que abra un archivo, la calificación de gravedad de la vulnerabilidad se reduce a 7.8, según el CVSS.

Sin embargo, desde una perspectiva práctica, engañar a los usuarios para que realicen la acción requerida no debería ser un gran desafío, y dado el gran tamaño de la base de usuarios de WinRAR, los atacantes tienen amplias oportunidades para una explotación exitosa.

El proveedor RARLAB actuó con rapidez al ser notificado de la vulnerabilidad, lanzando WinRAR versión 6.23 el 2 de agosto de 2023, que aborda efectivamente la vulnerabilidad. Es crucial que los usuarios de WinRAR apliquen esta actualización de seguridad tan pronto como sea posible para reducir la exposición al riesgo.

Aparte de la corrección del código de procesamiento de volúmenes de recuperación RAR4, la versión 6.23 soluciona un problema con archivos especialmente diseñados que conducen a un inicio de archivo incorrecto, que también se considera un problema de alta gravedad.

Microsoft también está haciendo cambios en el panorama de archivos RAR. Windows 11 está probando el soporte nativo para archivos RAR, 7-Zip y GZ.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible 6.23 que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2023/08/vulnerabilidad-en-winrar.html • hxxps://www.bleepingcomputer.com/news/security/winrar-flaw-lets-hackers-run-programs-when-you-open-rar-archives/