Se ha revelado una grave vulnerabilidad de seguridad de alto nivel en la utilidad WinRAR que podría ser potencialmente aprovechada por un actor malicioso para lograr la ejecución de código remoto en sistemas Windows.

Identificada como CVE-2023-40477 (con una puntuación CVSS de 7.8), la vulnerabilidad se ha descrito como un caso de validación inadecuada durante el procesamiento de volúmenes de recuperación.

> *«El problema se deriva de la falta de una adecuada validación de los datos proporcionados por el usuario, lo que puede dar lugar a un acceso a la memoria más allá del límite de un búfer asignado»*, advirtió la Iniciativa de Día Cero (ZDI) en un aviso.

> *«Un atacante podría aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual».*

Para explotar con éxito la vulnerabilidad, se requiere la interacción del usuario, ya que el objetivo debe ser persuadido para visitar una página maliciosa o simplemente abrir un archivo de archivo trampa.

Un investigador de seguridad, que utiliza el alias goodbyeselene, ha sido reconocido por descubrir y reportar la falla el 8 de junio de 2023. El problema se ha solucionado en la versión 6.23 de WinRAR, lanzada el 2 de agosto de 2023.

> *«Se ha abordado un problema de seguridad relacionado con la escritura fuera de límites en el código de procesamiento de volúmenes de recuperación RAR4»,* indicaron los responsables del software.

La versión más reciente también resuelve un segundo problema en el que *«WinRAR podría abrir un archivo incorrecto después de que un usuario hiciera doble clic en un elemento en un archivo especialmente diseñado»*. El investigador de Group-IB, Andrey Polovinkin, ha sido acreditado por reportar este problema.

Se recomienda a los usuarios actualizar a la versión más reciente para reducir los riesgos de posibles amenazas.