Investigadores de seguridad informática descubrieron una nueva vulnerabilidad de ejecución remota de código peligrosa en el software WinRAR, que afecta a cientos de millones de usuarios en todo el mundo.

Los investigadores de seguridad cibernética en Check Point revelaron detalles técnicos de una vulnerabilidad crítica en WinRAR, una popular aplicación de compresión de archivos de Windows con 500 millones de usuarios en todo el mundo, que afecta a todas las versiones del software lanzado en los últimos 19 años.

El fallo reside en la forma en que una antigua biblioteca de terceros, llamada UNACEV2.DLL, utilizada por el software que maneja la extracción de archivos comprimidos en formato de archivos de datos ACE.

Sin embargo, ya que WinRAR detecta el formato por el contenido del archivo y no por la extensión, los atacantes pueden simplemente cambiar la extensión .ace a la extensión .rar para verse normal.

Según los investigadores, lograron encontrar un error *«Absolute Path Traversal»* en la biblioteca que podría aprovecharse para ejecutar código arbitrario en un sistema específico que intenta descomprimir un archivo malintencionado utilizando las versiones vulnerables de WinRAR.

La falla de la ruta de acceso permite a los atacantes extraer archivos comprimidos en una carpeta de su elección en lugar de la carpeta elegida por el usuario, lo que brinda la oportunidad de colocar código malicioso en la carpeta de inicio de Windows, donde se ejecutará automáticamente en el siguiente reinicio.

En el siguiente video compartido por los investigadores, se observa que para poder tomar el control total de las computadoras seleccionadas, el atacante solo debe convencer a los usuarios de que solo abran archivos comprimidos malintencionados con WinRAR.

Como el equipo de WinRAR perdió el código fuente de la biblioteca UNACEV2.dll en 2005,

decidió eliminar UNACEV2.dll de su paquete para solucionar el problema y lanzó la versión 5.70 beta 1 de WinRAR que no es compatible con el formato ACE.

Se recomienda a los usuarios de Windows que instalen la última versión de WinRAR tan pronto como sea posible y eviten abrir archivos recibidos de fuentes desconocidas.

O quizás sea tiempo de ver otras alternativas a WinRAR que podrían gustarte más.