Se ha divulgado una vulnerabilidad crítica de seguridad en la herramienta de limpieza y transformación de datos de código abierto OpenRefine que podría llevar a cabo la ejecución de código arbitrario en sistemas afectados.

Identificada como CVE-2023-37476 (calificación CVSS: 7.8), la vulnerabilidad es una debilidad de tipo *«Zip Slip»* que podría tener consecuencias graves al importar un proyecto especialmente elaborado en versiones 3.7.3 y anteriores.

> *«A pesar de que OpenRefine está diseñado para funcionar únicamente en el equipo local del usuario, un atacante podría engañar al usuario para que importe un archivo de proyecto malicioso. Una vez que este archivo se importa, el atacante puede ejecutar código arbitrario en el equipo del usuario»*, informó Stefan Schiller, investigador de seguridad de Sonar, en un informe publicado la semana pasada.

El software propenso a vulnerabilidades de «Zip Slip» puede abrir la puerta a la ejecución de código aprovechando un fallo de travesía de directorios que un atacante puede explotar para acceder a partes del sistema de archivos que, en condiciones normales, estarían fuera de su alcance.

El ataque se basa en dos componentes en movimiento: un archivo malicioso y código de extracción que no realiza una comprobación de validación adecuada, lo que podría permitir la sobrescritura de archivos o su descompresión en ubicaciones no previstas.

Los archivos extraídos pueden ser invocados ya sea de forma remota por el atacante o por el sistema (o usuario), lo que resulta en la ejecución de comandos en el equipo de la víctima.

La vulnerabilidad detectada en OpenRefine sigue una línea similar, ya que el método «untar» para extraer los archivos del archivo permite a un actor malintencionado escribir archivos fuera de la carpeta de destino mediante la creación de un archivo con el nombre *«../../../../tmp/pwned»*.

Después de una divulgación responsable el 7 de julio de 2023, la vulnerabilidad se ha solucionado en la versión 3.7.4, que se publicó el 17 de julio de 2023.

> *«Esta vulnerabilidad proporciona a los atacantes un recurso poderoso: escribir archivos con contenido arbitrario en una ubicación arbitraria del sistema de archivos»*, indicó Schiller.

> *«Para aplicaciones que se ejecutan con privilegios de administrador, existen numerosas posibilidades para convertir esto en una ejecución de código arbitrario en el sistema operativo: agregar un nuevo usuario al archivo passwd, agregar una clave SSH, crear una tarea programada y mucho más».*

Esta divulgación se produce al mismo tiempo que ha aparecido código de explotación de prueba de concepto (PoC) para un par de vulnerabilidades ya corregidas en Microsoft SharePoint Server, CVE-2023-29357 (calificación CVSS: 9.8) y CVE-2023-24955 (calificación CVSS: 7.2), que podrían combinarse para lograr la escalada de privilegios y la ejecución de código remoto.

Además, sigue una alerta de Cyfirma sobre una vulnerabilidad crítica en Apache NiFi (CVE-2023-34468, calificación CVSS: 8.8) que permite la ejecución de código remoto mediante cadenas de conexión maliciosas a la base de datos H2. Esta vulnerabilidad se ha resuelto en Apache NiFi 1.22.0.

> *«El impacto de esta vulnerabilidad es grave, ya que concede a los atacantes la capacidad de acceder sin autorización a sistemas, extraer datos confidenciales y ejecutar código malicioso de forma remota. Un atacante podría aprovechar esta vulnerabilidad para comprometer la integridad de los datos, interrumpir operaciones y potencialmente causar daños financieros y daños a la reputación»*,

> advirtió la firma de ciberseguridad.