Investigadores de seguridad cibernética revelaron detalles de dos vulnerabilidades de seguridad en el software de código abierto ImageMagick que podrían conducir a una denegación de servicio (DoS) y divulgación de información.

Las dos vulnerabilidades, que fueron identificadas por la compañía latinoamericana de seguridad, Metabase Q, en la versión 7.1.0-49, se abordaron en la versión 7.1.0-52 de ImageMagick, lanzada en noviembre de 2022.

Una breve descripción de las vulnerabilidades es la siguiente:

- CVE-2022-44267: Una vulnerabilidad DoS que surge al analizar una imagen PNG con un nombre de archivo que es un solo guión («-«).
- CVE-2022-44268: Una vulnerabilidad de divulgación de información que podría explotarse para leer archivos arbitrarios de un servidor al analizar una imagen.

Un atacante debe poder cargar una imagen maliciosa en un sitio web utilizando ImageMagick para convertir las fallas en armas de forma remota. La imagen especialmente diseñada, por su parte, se puede crear insertando un fragmento de texto que especifica algunos metadatos elegidos por el atacante.

> *«Aunque el nombre de archivo especificado es '-', ImageMagick intentará leer el contenido de la entrada estándar, lo que podría dejar el proceso esperando para siempre»,* dijeron los investigadores en un informe.

De la misma forma, si el nombre del archivo hace referencia a un archivo real ubicado en el servidor (por ejemplo, «/etc/passwd/»), una operación de procesamiento de imágenes realizada en la entrada podría potencialmente incrustar el contenido del archivo remoto en la imagen procesada después de que esté completo.

Esta no es la primera vez que se descubren vulnerabilidades de seguridad en ImageMagick. En mayo de 2016, se revelaron múltiples vulnerabilidades en el software, una de las cuales,

denominada ImageTragick, podría haber sido objeto de abuso para obtener la ejecución remota de código al procesar imágenes enviadas por los usuarios.

Después, se reveló una vulnerabilidad de inyección de shell en noviembre de 2020, en la que un atacante podría insertar comandos arbitrarios al convertir archivos PDF cifrados en imágenes a través del parámetro de línea de comando «-authenticate».