Los investigadores de seguridad cibernética revelaron un problema que podría haber permitido a los atacantes armar la plataforma VirusTotal como un conducto para lograr la ejecución remota de código (RCE) en máquinas de sandboxing de terceros sin parques que empleaban motores antivirus.

La vulnerabilidad, ya parcheada, hizo posible *«ejecutar comandos de forma remota por medio de la plataforma VirusTotal y obtener acceso a sus diversas capacidades de escaneo»,* dijeron los investigadores de Cysource, Shai Alfasi y Marlon Fabiano da Silva.

VirusTotal, parte de la subsidiaria de seguridad Chronicle de Google, es un servicio de escaneo de malware que analiza archivos y URL sospechosos y busca virus utilizando más de 70 productos antivirus de terceros.

El método de ataque consistía en cargar un archivo DjVu a través de la interfaz de usuario web de la plataforma, que cuando se pasaba a varios motores de escaneo de malware de terceros, podía desencadenar un exploit para una vulnerabilidad de ejecución remota de código de alta gravedad en ExifTool, una utilidad de código abierto utilizada para leer y editar información de metadatos EXIF en archivos de imagen y PDF.

Rastreada como CVE-2021-22204 (puntaje CVSS: 7.8), la vulnerabilidad de alta gravedad es un caso de ejecución de código arbitrario que surge del mal manejo de los archivos DjVu por parte de ExifTool. El problema fue solucionado por sus mantenedores en una actualización de seguridad lanzada el 13 de abril de 2021.

Una consecuencia de esta explotación, según los investigadores, fue que otorgó un shell inverso a las máquinas afectadas vinculadas a algunos motores antivirus que aún no habían sido parcheados para la vulnerabilidad de ejecución remota de código.

Cabe mencionar que la vulnerabilidad no afecta a VirusTotal, y en un comunicado, Bernardo

Quintero, su fundador, confirmó que es el comportamiento previsto y que las ejecuciones de código no están en la plataforma en sí sino en los sistemas de escaneo de terceros que analizan y ejecutan las muestras. La compañía también dijo que está usando una versión de ExifTool que no es vulnerable a la falla.

Cysource dijo que informó de forma responsable el error a través de los Programas de Recompensa por Vulnerabilidad (VRP) de Google el 30 de abril de 2021, luego de lo cual, la vulnerabilidad de seguridad se corrigió inmediatamente.

Esta no es la primera vez que la vulnerabilidad ExifTool surge como un conducto para lograr la ejecución remota de código. El año pasado, GitLab solucionó una falla crítica (CVE-2021-22205, puntaje CVSS: 10) relacionada con una validación incorrecta de las imágenes proporcionadas por el usuario, lo que llevó a la ejecución de código arbitrario.