Un individuo malicioso ha divulgado un falso exploit de prueba de concepto (PoC) para una reciente vulnerabilidad de WinRAR en GitHub, con la intención de infectar a aquellos usuarios que descargaron el código con el malware Venom RAT.

> *«El PoC falso diseñado para aprovechar esta vulnerabilidad de WinRAR se basó en un guión PoC de acceso público que explotaba una vulnerabilidad de inyección SQL en una aplicación denominada GeoServer, identificada como CVE-2023-25157»,* afirmó el investigador de Palo Alto Networks Unit 42, Robert Falcone.

Aunque los PoCs falsos son una estratagema ampliamente documentada para apuntar a la comunidad de investigación, la firma de ciberseguridad sospechó que los actores maliciosos estaban buscando aprovechar oportunidades para dirigirse a otros delincuentes que podrían estar incorporando las últimas vulnerabilidades en su arsenal.

La cuenta de GitHub que alojaba el repositorio, bajo el nombre de whalersplonk, ya no está disponible. Se ha informado que el PoC fue publicado el 21 de agosto de 2023, cuatro días después de que se hiciera público el anuncio sobre la vulnerabilidad.

CVE-2023-40477 se relaciona con un problema de validación inadecuada en la utilidad WinRAR que podría ser aprovechado para lograr la ejecución remota de código (RCE) en sistemas Windows. Fue corregido el mes pasado por los administradores en la versión WinRAR 6.23, junto con otra vulnerabilidad que estaba siendo explotada activamente, identificada como CVE-2023-38831.

Un análisis del repositorio revela un guión en Python y un vídeo de Streamable que muestra cómo utilizar el exploit. El vídeo atrajo un total de 121 visualizaciones.

En lugar de ejecutar el PoC, el guión en Python se comunica con un servidor remoto (checkblacklistwords[.]eu) para obtener un archivo ejecutable llamado Windows.Gaming.Preview.exe, que es una variante de Venom RAT. Este programa tiene la capacidad de listar procesos en ejecución y recibir órdenes de un servidor controlado por el

actor (94.156.253[.]109).

Una inspección más detallada de la infraestructura de ataque muestra que el actor malicioso creó el dominio checkblacklistwords[.]eu al menos 10 días antes de que se hiciera pública la vulnerabilidad, y luego aprovechó rápidamente la importancia de la falla para atraer posibles víctimas.

> *«Un actor malicioso desconocido intentó comprometer a individuos al divulgar un falso PoC después del anuncio público de la vulnerabilidad, con el objetivo de explotar una vulnerabilidad de ejecución remota de código (RCE) en una aplicación ampliamente conocida. Este PoC es falso y no aprovecha la vulnerabilidad de WinRAR, lo que sugiere que el actor intentó aprovechar una RCE muy solicitada en WinRAR para comprometer a otros»,* declaró Falcone.