Más del 50% de los 90,310 anfitriones han sido detectados exponiendo un servicio Tinyproxy en la red que presenta una grave vulnerabilidad de seguridad no parcheada en la herramienta proxy HTTP/HTTPS.

El problema, identificado como CVE-2023-49606, cuenta con una puntuación CVSS de 9.8 sobre 10, según Cisco Talos, que lo ha descrito como un error de liberación de memoria después de su uso que afecta a las versiones 1.10.0 y 1.11.1, siendo esta última la más actual.

> *«Un encabezado HTTP especialmente diseñado puede desencadenar la reutilización de memoria previamente liberada, lo que provoca una corrupción de la memoria y podría resultar en la ejecución remota de código. Un atacante necesita realizar una solicitud HTTP no autenticada para activar esta vulnerabilidad»,* informó Talos en un aviso la semana pasada.

En otras palabras, un actor de amenazas no autenticado podría enviar un encabezado de Conexión HTTP especialmente manipulado para provocar una corrupción de la memoria que podría derivar en la ejecución remota de código.

Según los datos proporcionados por la empresa de gestión de superficie de ataque Censys, de los 90,310 anfitriones que exponen un servicio Tinyproxy en internet público hasta el 3 de mayo de 2024, 52,000 (~57%) de ellos están ejecutando una versión de Tinyproxy vulnerable.

La mayoría de los anfitriones accesibles públicamente se encuentran en Estados Unidos (32,846), Corea del Sur (18,358), China (7,808), Francia (5,208) y Alemania (3,680).

Talos, que reportó el problema el 22 de diciembre de 2023, también ha lanzado una demostración de concepto (PoC) para la falla, describiendo cómo el problema con el análisis de conexiones HTTP Connection podría ser explotado para provocar un fallo y, en algunos casos, la ejecución de código.

Los responsables de mantener Tinyproxy, en una serie de commits realizados durante el fin de semana, criticaron a Talos por enviar el informe a una *«dirección de correo electrónico probablemente desactualizada»*, añadiendo que se enteraron de ello por un mantenedor del paquete Tinyproxy de Debian el 5 de mayo de 2024.

> *«No se abrió ningún problema en GitHub, y nadie mencionó una vulnerabilidad en el chat IRC mencionado. Si el problema se hubiera reportado en GitHub o IRC, el error se habría solucionado en un día»,* afirmó rofl0r en un compromiso.

Se recomienda a los usuarios que actualicen a la última versión en cuanto esté disponible. También se aconseja no exponer el servicio Tinyproxy en internet público.