Al parecer, hasta 350,000 proyectos de código abierto son potencialmente vulnerables a la explotación como resultado de una vulnerabilidad de seguridad en un módulo de Python que no ha sido parcheado por 15 años.

Los repositorios de código abierto abarcan una serie de verticales de la industria, como desarrollo de software, inteligencia artificial, aprendizaje automático, desarrollo web, medios, seguridad y gestión de TI.

La vulnerabilidad, rastreada como CVE-2007-4559 (puntaje CVSS: 6.8), tiene sus raíces en el módulo tarfile, cuya explotación exitosa podría conducir a la ejecución de código desde una escritura de archivo arbitraria.

> *«La vulnerabilidad es un ataque transversal de ruta en las funciones extract y extractall en el módulo tarfile que permite a un atacante sobrescribir archivos arbitrarios agregando la secuencia '..' a los nombres de archivo en un archivo TAR»,* dijo el investigador de seguridad de Trellix, Kasimir Schulz.

Revelado originalmente en agosto de 2007, el error tiene que ver con cómo se puede aprovechar un archivo tar especialmente diseñado para sobrescribir archivos arbitrarios en una máquina de destino simplemente con abrir el archivo.

En pocas palabras, un actor de amenazas puede explotar la vulnerabilidad al cargar un archivo tar malicioso de una forma que hace posible escapar del directorio en el que se pretende extraer un archivo y lograr la ejecución del código, lo que permite al atacante potencialmente tomar el control de un dispositivo objetivo.

> *«Nunca extraiga archivos de fuentes no confiables sin una inspección previa. Es posible que los archivos se creen fuera de la ruta, por ejemplo, miembros que tienen nombres de archivo absolutos que comienzan con '/' o nombres de archivo*

> *con dos puntos '..*'», dice la documentación de Python para tarfile.

La vulnerabilidad también recuerda una falla de seguridad revelada recientemente en la utilidad UnRAR de RARlab (CVE-2022-30333) que podría conducir a la ejecución remota de código.

Trellix lanzó además una utilidad personalizada llamada Creosote, para buscar proyectos vulnerables a CVE-2007-4559, utilizándola para descubrir la vulnerabilidad en el IDE de Spyder Python, así como el Polemarch.

> *«Si no se controla, esta vulnerabilidad se ha agregado involuntariamente a cientos de miles de proyectos de código abierto y cerrado en todo el mundo, creando una superficie de ataque sustancial en la cadena de suministro de software»,* dijo Douglas McKee.