Un investigador de seguridad alemán reveló públicamente detalles sobre una grave vulnerabilidad en una de las aplicaciones de servidor FTP más populares, que potencialmente podría afectar a más de un millón de servidores.

El software vulnerable es ProFTPD, un servidor FTP de código abierto que es utilizado por una gran cantidad de empresas y sitios web populares, incluyendo SourceForge, Samba y Slackware, y viene preinstalado en muchas distribuciones de Linux y Unix, como Debian.

Descubierta por Tobias Mädel, la vulnerabilidad reside en el módulo mod_copy de la aplicación ProFTPD, un componente que permite a los usuarios copiar archivos o directorios de un lugar a otro en un servidor sin tener que transferir los datos al cliente y viceversa.

Según Mädel, un problema de control de acceso incorrecto en el módulo mod_copy podría explotarse para copiar de forma no autorizada cualquier archivo en el servidor FTP, lo que podría provocar ataques remotos de ejecución de código y divulgación de información.

La vulnerabilidad, asignada como CVE-2019-12815, afecta a todas las versiones de ProFTPD, incluida la última versión 1.3.6 que se lanzó en 2017.

Como el módulo mod_copy viene deshabilitado de forma predeterminada en la mayoría de los sistemas operativos que utilizan ProFTPD, la falla podría afectar a una gran cantidad de servidores expuestos en Internet, como lo muestra un informe del motor de búsqueda Shodan.

Según un aviso, el problema que apenas fue descubierto está relacionado con una vulnerabilidad parecida de hace 4 años (CVE-2015-3306) en el módulo mod_copy, que permite a los atacantes remotos leer y escribir en archivos arbitrarios por medio de los comandos CPFR y CPTO del sitio.

Sin embargo, el investigador detalló que la falla de 2015 era *«mucho más peligrosa»* que la nueva. Mädel informó sobre la vulnerabilidad a los desarrolladores del proyecto ProFTPD en septiembre del año pasado, pero el equipo no tomó medidas para resolver el problema por

más de 9 meses.

Por lo tanto, el investigador contactó al equipo de seguridad de Debian el mes pasado, luego de esto, el equipo de ProFTPD finalmente creó un parche y la semana pasada lo liberó en la versión 1.3.6 sin lanzar una nueva versión de su servidor FTP.

Como solución alternativa, los administradores de servidores también pueden deshabilitar el módulo mod_copy en el archivo de configuración ProFTPD para protegerse de ser víctimas de cualquier ataque relacionado con la falla.