Los administradores del cliente de Secure Shell (SSH) y Telnet PuTTY están avisando a los usuarios sobre una vulnerabilidad crítica que afecta a las versiones desde la 0.68 hasta la 0.80 y que podría ser explotada para obtener acceso completo a las claves privadas NIST P-521 (ecdsa-sha2-nistp521).

Esta falla ha sido identificada con el código CVE-2024-31497, y su descubrimiento ha sido atribuido a los investigadores Fabian Bäumer y Marcus Brinkmann de la Universidad de Ruhr en Bochum.

«El impacto de esta vulnerabilidad es comprometer la clave privada», explicó el proyecto PuTTY en un aviso.

> *«Un atacante que tenga acceso a algunos mensajes firmados y la clave pública podría obtener suficiente información para recuperar la clave privada y falsificar firmas como si fueran tuyas, lo que les permitiría, por ejemplo, acceder a cualquier servidor en el que utilices dicha clave».*

Sin embargo, para obtener las firmas, un atacante tendría que comprometer el servidor al que se accede con dicha clave.

En un mensaje publicado en la lista de correo Open Source Software Security (oss-sec), Bäumer detalló que la falla surge de la generación de nonces criptográficos ECDSA con sesgos, lo que posibilitaría la recuperación de la clave privada.

> *«Los primeros 9 bits de cada nonce ECDSA son cero. Esto permite recuperar completamente la clave secreta en aproximadamente 60 firmas mediante técnicas de vanguardia»*, explicó Bäumer.
>
> *«Estas firmas pueden ser recolectadas por un servidor malicioso (los ataques de*

> *intermediarios no son posibles dado que los clientes no transmiten sus firmas de manera clara) o desde cualquier otra fuente, como commits de git firmados a través de agentes reenviados».*

Además de afectar a PuTTY, esta vulnerabilidad también impacta a otros productos que incorporan una versión vulnerable del software:

- FileZilla (3.24.1 – 3.66.5)
- WinSCP (5.9.5 – 6.3.2)
- TortoiseGit (2.4.0.2 – 2.15.0)
- TortoiseSVN (1.10.0 – 1.14.6)

Tras la divulgación responsable, el problema ha sido resuelto en PuTTY 0.81, FileZilla 3.67.0, WinSCP 6.3.3 y TortoiseGit 2.15.0.1. Se recomienda a los usuarios de TortoiseSVN que utilicen Plink de la última versión de PuTTY 0.81 al acceder a un repositorio SVN a través de SSH hasta que esté disponible un parche.

En concreto, se ha solucionado cambiando a la técnica RFC 6979 para todos los tipos de claves DSA y ECDSA, abandonando el método anterior de derivación del nonce mediante un enfoque determinista que, aunque evitaba la necesidad de una fuente de aleatoriedad de alta calidad, era susceptible a nonces sesgados cuando se usaba P-521.

Además, las claves ECDSA NIST-P521 utilizadas con cualquiera de los componentes vulnerables deben considerarse comprometidas y, por lo tanto, revocadas eliminándolas de los archivos ~/.ssh/authorized_keys y sus equivalentes en otros servidores SSH.