Los expertos en seguridad de la Universidad de Ruhr en Bochum han identificado una debilidad en el protocolo de comunicación segura Secure Shell (SSH) que podría ser explotada para reducir la protección de una conexión, comprometiendo la integridad del canal seguro.

Este problema, denominado Terrapin (CVE-2023-48795, con una calificación CVSS de 5.9), se ha etiquetado como el *«primer ataque de reducción de prefijo que puede ser aprovechado en la práctica».*

> - Los investigadores Fabian Bäumer, Marcus Brinkmann y Jörg Schwenk explicaron: *«Manipulando los números de secuencia durante el intercambio inicial, un atacante podría omitir ciertos mensajes enviados al inicio de la comunicación sin que ninguno de los extremos lo detecte».*

SSH es un sistema que permite enviar instrucciones de manera protegida a un equipo a través de una red insegura, basándose en técnicas criptográficas para verificar y cifrar las comunicaciones entre dispositivos.

Para establecer esta comunicación segura, las partes involucradas en la conexión, el cliente y el servidor, coordinan un proceso inicial donde se establecen los parámetros criptográficos y se intercambian las claves necesarias para garantizar la confidencialidad y la integridad.

No obstante, un atacante con acceso a la red y la habilidad de intervenir y alterar el tráfico puede manipular el proceso de negociación del SSH, debilitando la seguridad del sistema.

> Los investigadores añadieron: *«Esta técnica de manipulación puede permitir que se utilicen métodos de autenticación menos robustos y se desactiven ciertas protecciones contra amenazas específicas en versiones de OpenSSH 9.5».*

Un aspecto clave para que este ataque sea exitoso es que la conexión esté utilizando modos

de cifrado vulnerables, como ChaCha20-Poly1305 o CBC con Encrypt-then-MAC.

> Qualys advirtió sobre los riesgos asociados: *«En situaciones reales, un ciberdelincuente podría aprovechar esta brecha para acceder a información delicada o comprometer sistemas vitales con privilegios elevados. Las organizaciones con redes extensas y complejas son especialmente vulnerables».*

Esta vulnerabilidad afecta a numerosas implementaciones de SSH, incluyendo OpenSSH, Paramiko, PuTTY, KiTTY, WinSCP, libssh, libssh2, AsyncSSH, FileZilla y Dropbear. Los responsables de estas herramientas han lanzado actualizaciones para corregir este problema.

> Yair Mizrahi, experto en seguridad de JFrog, comentó: *«Dado que SSH y, en particular, OpenSSH son esenciales en muchas aplicaciones empresariales en la nube, es crucial que las empresas se aseguren de proteger sus sistemas. Pero también es importante recordar que un cliente vulnerable puede comprometer una conexión, por lo que las organizaciones deben estar alerta y tomar medidas correctivas rápidamente».*