Un reciente estudio ha evidenciado la posibilidad de que atacantes de red pasivos obtengan claves privadas de host RSA desde un servidor SSH vulnerable al observar fallas computacionales naturales que se producen durante el establecimiento de la conexión.

El protocolo Secure Shell (SSH) es un método para transmitir comandos e iniciar sesión de forma segura en una computadora a través de una red no segura. Basado en una arquitectura cliente-servidor, SSH utiliza técnicas criptográficas para autenticar y cifrar conexiones entre dispositivos.

Una clave de host es una clave criptográfica utilizada para autenticar computadoras en el protocolo SSH. Estas claves son pares que generalmente se generan mediante sistemas criptográficos de clave pública como RSA.

> Un grupo de académicos de la Universidad de California, San Diego, y del Instituto de Tecnología de Massachusetts, expresó en un informe de este mes: *«Si una implementación de firma que utiliza CRT-RSA presenta una falla durante el cálculo de la firma, un atacante que observe esta firma podría tener la capacidad de calcular la clave privada del firmante».*

En otras palabras, un adversario pasivo puede monitorear silenciosamente conexiones legítimas sin riesgo de detección hasta que observe una firma defectuosa que revele la clave privada. El actor malintencionado podría entonces hacerse pasar por el host comprometido para interceptar datos sensibles y llevar a cabo ataques de intermediario en el medio (AitM).

Los investigadores describieron el método como un ataque de falla de recuperación de clave basado en retículas, que les permitió recuperar las claves privadas correspondientes a 189 claves públicas RSA únicas, posteriormente rastreadas hasta dispositivos de cuatro fabricantes: Cisco, Hillstone Networks, Mocana y Zyxel.

Cabe destacar que el lanzamiento de la versión 1.3 de TLS en 2018 actúa como contramedida al cifrar el saludo que establece la conexión, evitando así que observadores

pasivos accedan a las firmas.

> *«Estos ataques ilustran de manera concreta el valor de varios principios de diseño en criptografía: cifrar los saludos del protocolo tan pronto como se negocia una clave de sesión para proteger los metadatos, vincular la autenticación a una sesión y separar la autenticación de las claves de cifrado»*, señalaron los investigadores.

Estos hallazgos surgen dos meses después de la divulgación del Ataque Marvin, una variante del Ataque ROBOT (acrónimo de *«Return Of Bleichenbacher's Oracle Threat»*) que permite a un actor de amenazas descifrar textos cifrados RSA y falsificar firmas mediante la explotación de debilidades de seguridad en PKCS #1 v1.5.