[notasdeprensa.jpg](http://www.mexicopress.com.mx)Publicado en América Latina el 28/03/2024

# [Cómo pueden extraer las claves RSA los hackers según DigiCert](http://www.notasdeprensa.es)

## Dean Coclin, director senior en desarrollo empresarial de Digicert, analiza los aspectos más importantes de este asunto

En meses pasados, The Hacker News publicó un artículo que cita una investigación académica publicada en noviembre de 2023 titulado "Compromiso de clave SSH pasiva a través de celosías". La investigación describió una técnica hipotética que podría usarse para extraer claves RSA privadas si estuvieran presentes todas las condiciones siguientes: Primero, se monitorea y establece un patrón de conexiones confiables. En segundo lugar, una anomalía que identifican como una falla computacional que ocurre naturalmente genera una firma defectuosa. En tercer lugar, la firma defectuosa antes mencionada se verifica por error como si fuera confiable. Además, el software utilizado no permite ni emplea un sistema de señalización automatizado para identificar fallas de firma antes de intentar establecer conexiones. Luego, debe estar presente un parámetro específico, aunque comúnmente utilizado, para las claves SSH. La investigación sugiere que, en estas condiciones, pudieron descubrir 189 claves comprometidas en la naturaleza porque se implementaron con estas vulnerabilidades específicas. Damos la bienvenida a esta y a todas las investigaciones que mejoren los estándares de confianza digital en cada ecosistema. Con la adquisición de Mocana, que fue citada junto con Cisco, Hillstone Networks y Zyxel como las marcas cuyos clientes pueden haber implementado esta rara vulnerabilidad, se están tomando esta investigación muy en serio y ya han tomado contramedidas para prevenir tal ataque, sin importar cuán raro sea. Las implicaciones de la criptoagilidadLa investigación subraya la necesidad de adoptar un paradigma cripto-ágil y prácticas de cripto-agilidad, particularmente para cualquiera que todavía use cualquier versión de TLS anterior a TLS 1.3 que se implementó en 2018. Los últimos algoritmos y técnicas son la mejor contramedida. Cualquier noción de prácticas criptográficas de "configúrelo y olvídese" socavará la confianza digital y potencialmente expondrá vulnerabilidades con el tiempo, especialmente a medida que la computación cuántica se convierta en una realidad. Las implicaciones poscuánticasEs probable que este tipo de investigación aumente en frecuencia y gravedad a medida que la computación cuántica se vuelva más estable y acelere las pruebas y el descifrado de algoritmos matemáticos complicados. Las organizaciones deberán reaccionar más rápidamente ante posibles vulnerabilidades en sus ecosistemas. Para prepararse para la criptografía poscuántica o PQC, se deben tomar medidas de inmediato para descubrir, identificar y mapear un libro de registro completo para todos los activos criptográficos. Deben existir herramientas de automatización para rotar certificados y claves para lograr agilidad criptográfica.

**Datos de contacto:**

Prensa DigiCert

PR Latam DigiCert

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/como-pueden-extraer-las-claves-rsa-los-hackers\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional Telecomunicaciones Programación Software Ciberseguridad Innovación Tecnológica

[notasdeprensa.jpg](http://www.mexicopress.com.mx)

[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)