Google ha informado que cambiará de KYBER a ML-KEM en su navegador Chrome, como parte de sus esfuerzos continuos para protegerse del riesgo de las computadoras cuánticas relevantes para la criptografía (CRQCs).

> *«Chrome ofrecerá una predicción de clave para el sistema híbrido ML-KEM (código 0x11EC). La bandera `PostQuantumKeyAgreementEnabled` y la política empresarial aplicarán tanto a Kyber como a ML-KEM»*, comentaron David Adrian, David Benjamin, Bob Beck y Devon O'Brien del equipo de Chrome.

Se espera que estos cambios se implementen en la versión 131 de Chrome, que está programada para su lanzamiento a principios de noviembre de 2024. Google también destacó que ambos enfoques híbridos de intercambio de claves post-cuántico no son compatibles entre sí, lo que ha llevado a la empresa a descartar KYBER.

> *«Las modificaciones en la versión final de ML-KEM lo hacen incompatible con la versión previamente implementada de Kyber. Por esta razón, el código TLS para el intercambio híbrido de claves post-cuánticas cambiará de 0x6399 para Kyber768+X25519 a 0x11EC para ML-KEM768+X25519»*, señaló la empresa.

Este desarrollo llega poco después de que el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. publicara las versiones finales de tres nuevos algoritmos de cifrado, diseñados para proteger los sistemas actuales de futuros ataques cuánticos, culminando un esfuerzo de ocho años de la agencia.

Los algoritmos mencionados son FIPS 203 (también conocido como ML-KEM), FIPS 204 (también conocido como CRYSTALS-Dilithium o ML-DSA) y FIPS 205 (también conocido como Sphincs+ o SLH-DSA), que se utilizarán para cifrado general y protección de firmas digitales. Un cuarto algoritmo, FN-DSA (originalmente llamado FALCON), está programado para ser finalizado más adelante este año.

ML-KEM, que significa Mecanismo de Encapsulación de Clave basado en Redes Modulares, deriva de la tercera fase del KEM CRYSTALS-KYBER y permite establecer una clave secreta compartida entre dos partes que se comunican a través de un canal público.

Microsoft, por su parte, también está preparando su transición al mundo post-cuántico con una actualización de su biblioteca criptográfica SymCrypt, que ahora incluirá soporte para ML-KEM y el Esquema de Firma Extendida de Merkle (XMSS).

«Incluir soporte para algoritmos post-cuánticos en el motor criptográfico subyacente es el primer paso hacia un mundo seguro ante las amenazas cuánticas», declaró el gigante de Windows, subrayando que la transición a la criptografía post-cuántica (PQC) es un *«proceso complejo, que llevará varios años y requerirá múltiples iteraciones»* con una planificación cuidadosa.

Este anuncio también sigue al descubrimiento de una vulnerabilidad criptográfica en los microcontroladores de seguridad Infineon SLE78, Optiga Trust M y Optiga TPM, que podría permitir la extracción de claves privadas del Algoritmo de Firma Digital de Curva Elíptica (ECDSA) de los dispositivos de autenticación de hardware YubiKey.

Se cree que esta falla criptográfica en la biblioteca proporcionada por Infineon ha pasado desapercibida durante 14 años, afectando aproximadamente 80 evaluaciones de certificación de Common Criteria de alto nivel.

El ataque de canal lateral, bautizado como EUCLEAK (CVE-2024-45678, puntuación CVSS: 4.9) por Thomas Roche de NinjaLab, afecta a todos los microcontroladores de seguridad de Infineon que integran la biblioteca criptográfica y a los siguientes dispositivos YubiKey:

- Versiones de la Serie YubiKey 5 anteriores a la 5.7
- Serie YubiKey 5 FIPS anteriores a la 5.7
- Serie YubiKey 5 CSPN anteriores a la 5.7
- Versiones de la Serie YubiKey Bio anteriores a la 5.7.2
- Todas las versiones de la Serie Security Key anteriores a la 5.7

- Versiones de YubiHSM 2 anteriores a la 2.4.0
- Versiones de YubiHSM 2 FIPS anteriores a la 2.4.0

> *«El atacante necesitaría tener en su poder la YubiKey, Security Key o YubiHSM, conocer las cuentas objetivo y contar con equipo especializado para ejecutar el ataque»,* explicó Yubico, la empresa responsable de YubiKey, en un comunicado coordinado.
>
> *«Dependiendo del caso de uso, el atacante también podría necesitar información adicional, como nombre de usuario, PIN, contraseña de la cuenta o clave de autenticación [YubiHSM]».*

Sin embargo, debido a que los dispositivos YubiKey afectados por estas versiones vulnerables de firmware no pueden ser actualizados —una decisión de diseño intencional para maximizar la seguridad y evitar nuevas vulnerabilidades—, seguirán siendo vulnerables a EUCLEAK.

La empresa ha anunciado que retirará el soporte para la biblioteca criptográfica de Infineon, sustituyéndola por su propia biblioteca criptográfica en las versiones de firmware YubiKey f5.7 y YubiHSM 2.4.

Un ataque similar, dirigido a las llaves de seguridad Google Titan, fue demostrado por Roche y Victor Lomne en 2021, lo que permitió a actores maliciosos clonar los dispositivos al aprovechar un canal lateral electromagnético en el chip que contienen.

> *«El ataque [EUCLEAK] requiere acceso físico al elemento seguro (bastan unos pocos minutos de adquisiciones electromagnéticas locales) para extraer la clave secreta ECDSA. En el caso del protocolo FIDO, esto permitiría clonar el dispositivo FIDO»,* indicó Roche.