Google ha declarado sus intenciones de incorporar soporte para algoritmos de encriptación resistentes a la computación cuántica en su navegador Chrome, a partir de la versión 116.

> *«Chrome comenzará a respaldar X25519Kyber768 para establecer secretos simétricos en TLS, a partir de Chrome 116, y estará disponible mediante una opción en Chrome 115″*, expresó Devon O'Brien en una publicación difundida el jueves.

Kyber ha sido seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de Estados Unidos como el candidato para la encriptación general en un intento por combatir futuros ciberataques derivados del surgimiento de la computación cuántica. Kyber-768 equivale en seguridad aproximadamente a AES-192.

Ya Cloudflare, Amazon Web Services e IBM han adoptado este algoritmo de encriptación.

X25519Kyber768 es un algoritmo híbrido que combina el resultado de X25519, un algoritmo de curva elíptica ampliamente empleado para el acuerdo de claves en TLS, y Kyber-768 para crear una clave de sesión sólida que encripta las conexiones TLS.

> *«Los mecanismos híbridos como X25519Kyber768 brindan la flexibilidad para implementar y probar nuevos algoritmos resistentes a la computación cuántica, garantizando al mismo tiempo que las conexiones sigan protegidas por un algoritmo seguro ya existente»,* explicó O'Brien.

Aunque se prevé que pasen varios años, incluso décadas, antes de que las computadoras cuánticas presenten riesgos graves, ciertas formas de encriptación son susceptibles a un ataque denominado «*cosecha ahora, descifrado después*» (también conocido como descifrado retrospectivo), en el cual los actores maliciosos recolectan datos encriptados hoy con la esperanza de descifrarlos más adelante, cuando el criptoanálisis sea más sencillo debido a avances tecnológicos.

Aquí es donde entran en juego las computadoras cuánticas, ya que son capaces de realizar de manera eficiente ciertos cálculos de forma que pueden derrotar con facilidad las implementaciones criptográficas actuales.

> *«En TLS, aunque se considera que los algoritmos de encriptación simétrica que resguardan los datos en tránsito son seguros contra el criptoanálisis cuántico, no ocurre lo mismo con la forma en que se generan las claves simétricas»,* apuntó O'Brien.

> *«De modo que en Chrome, mientras más pronto actualicemos TLS para emplear claves de sesión resistentes a la computación cuántica, más temprano podremos proteger el tráfico de red del usuario contra futuros intentos de criptoanálisis cuántico».*

Empresas que se encuentren con problemas de incompatibilidad en sus dispositivos de red tras la implementación, se les aconseja desactivar temporalmente X25519Kyber768 en Chrome utilizando la política empresarial PostQuantumKeyAgreementEnabled, que estará disponible a partir de Chrome 116.

Esta evolución llega en un momento en el que Google ha anunciado un cambio en el ritmo de publicación de sus actualizaciones de seguridad para Chrome, pasando de ser quincenales a semanales, con el objetivo de reducir la ventana de ataque y abordar el creciente problema de la brecha en las correcciones, que permite a los actores maliciosos disponer de más tiempo para aprovechar las vulnerabilidades de día n y de día cero que son publicadas.

> *«Los actores malintencionados podrían potencialmente aprovechar la visibilidad que tienen sobre estas correcciones y desarrollar exploits para aplicar contra los usuarios del navegador que aún no han recibido la solución. Por eso consideramos*

> *que es de suma importancia lanzar las correcciones de seguridad lo más pronto posible, para minimizar esta 'brecha de parches'»*, explicó Amy Ressler, miembro del Equipo de Seguridad de Chrome.