El día martes, Google anunció la primera implementación de una llave de seguridad FIDO2 resistente a la computación cuántica como parte de su iniciativa de llaves de seguridad OpenSK.

> *«Esta implementación de hardware de código abierto optimizada utiliza un esquema de firma híbrida ECC/Dilithium novedoso que se beneficia de la seguridad proporcionada por ECC ante ataques estándar y de la resistencia que brinda Dilithium frente a ataques cuánticos»*, expresaron Elie Bursztein y Fabian Kaczmarczyck.

OpenSK es una implementación de código abierto en Rust para llaves de seguridad que soporta tanto los estándares FIDO U2F como FIDO2.

Esta novedad llega en menos de una semana después de que la compañía tecnológica anunciara sus planes de agregar compatibilidad con algoritmos de encriptación resistentes a la computación cuántica en Chrome 116, con el fin de establecer claves simétricas en conexiones TLS.

Esto también es parte de esfuerzos más amplios para cambiar a algoritmos criptográficos que puedan enfrentar ataques cuánticos en el futuro, lo que hace necesario incorporar tales tecnologías desde etapas tempranas para facilitar una implementación gradual.

> *«Afortunadamente, con la reciente estandarización de la criptografía de clave pública resistente a la computación cuántica, incluido el algoritmo Dilithium, ahora contamos con un camino claro para asegurar las llaves de seguridad frente a ataques cuánticos»*, expresó el gigante de búsqueda.

De manera similar al mecanismo híbrido de Chrome, que es una combinación de X25519 y Kyber-768, la implementación propuesta de la llave de seguridad FIDO2 por parte de Google

es una combinación del Algoritmo de Firma Digital de Curva Elíptica (ECDSA) y el algoritmo de firma resistente a la computación cuántica recientemente estandarizado, Dilithium.

Este esquema de firma híbrida, desarrollado en colaboración con ETH Zürich, es una implementación optimizada en Rust y que requiere solo 20 KB de memoria, lo que la hace idónea para ejecutarse en el hardware limitado de las llaves de seguridad.

La empresa manifestó que *«espera que esta implementación (o una variante de la misma) sea estandarizada como parte de la especificación de llaves FIDO2 y sea respaldada por los principales navegadores web, de modo que las credenciales de los usuarios puedan estar protegidas contra ataques cuánticos».*