Google Cloud ha presentado firmas digitales seguras contra ataques cuánticos dentro del Servicio de Gestión de Claves de Google Cloud (Cloud KMS) para claves generadas por software. Esta iniciativa busca reforzar la seguridad de los sistemas de cifrado ante la amenaza que representan las computadoras cuánticas avanzadas en el ámbito criptográfico.

Esta nueva capacidad, actualmente en fase de prueba, complementa los estándares de criptografía post-cuántica (PQC) desarrollados por el Instituto Nacional de Estándares y Tecnología (NIST), cuyas versiones finales se oficializaron en agosto de 2024.

> *"Nuestra estrategia para la integración de PQC en Cloud KMS contempla el soporte de los estándares de criptografía post-cuántica del NIST (FIPS 203, FIPS 204, FIPS 205 y los que se establezcan en el futuro), tanto en soluciones basadas en software (Cloud KMS) como en hardware (Cloud HSM)"*, indicó el equipo de Google Cloud.
>
> *"Gracias a esto, los clientes podrán realizar importación y gestión de claves con seguridad cuántica, así como ejecutar procesos de cifrado, descifrado y generación de firmas digitales."*

La compañía detalló que las implementaciones de software de estos estándares – FIPS 203 (conocido como ML-KEM), FIPS 204 (CRYSTALS-Dilithium o ML-DSA) y FIPS 205 (Sphincs+ o SLH-DSA) – estarán disponibles como soluciones de código abierto.

Además, Google Cloud está colaborando con fabricantes de Módulos de Seguridad de Hardware (HSM) y con socios del Administrador de Claves Externas (EKM) para habilitar el uso de criptografía resistente a la computación cuántica en toda su infraestructura.

El objetivo de adoptar la criptografía post-cuántica de manera anticipada es proteger los sistemas frente a una amenaza denominada "Capturar Ahora, Descifrar Después" (HNDL, por sus siglas en inglés). Este tipo de ataque implica que ciberdelincuentes recopilen información cifrada en la actualidad con la intención de descifrarla en el futuro, cuando las computadoras

cuánticas sean lo suficientemente avanzadas como para vulnerar los algoritmos y protocolos de intercambio de claves tradicionales.

> *"Aunque la llegada de esta amenaza aún puede tardar algunos años, las organizaciones que implementan infraestructuras con raíces de confianza a largo plazo o que firman firmware para dispositivos esenciales deberían comenzar a tomar medidas de mitigación desde ahora",* señalaron Jennifer Fernick y Andrew Foster de Google Cloud.
>
> *"Cuanto antes podamos fortalecer la seguridad de estas firmas, más sólida será la base de confianza del ecosistema digital."*

Las firmas digitales resistentes a la computación cuántica en Cloud KMS están disponibles en fase preliminar para ML-DSA-65 (FIPS 204) y SLH-DSA-SHA2-128S (FIPS 205). Además, se prevé que en el futuro se integre compatibilidad con esquemas híbridos a través de API, dependiendo de la evolución del consenso en la comunidad criptográfica.