Los expertos en ciberseguridad han identificado una «*seria falla de diseño*» en la característica de delegación a nivel de dominio (DWD) de Google Workspace, la cual podría ser aprovechada por actores malintencionados para facilitar la escalada de privilegios y obtener acceso no autorizado a las API de Workspace sin necesidad de contar con privilegios de superadministrador.

Según un informe técnico compartido por parte de la firma de ciberseguridad Hunters, la explotación de esta vulnerabilidad podría dar lugar al robo de correos electrónicos de Gmail, la exfiltración de datos de Google Drive u otras acciones no autorizadas dentro de las API de Google Workspace en todas las identidades dentro del dominio objetivo.

Esta debilidad de diseño, que sigue activa hasta la fecha, ha sido denominada como DeleFriend debido a su habilidad para manipular las delegaciones existentes en la Plataforma Google Cloud (GCP) y Google Workspace sin necesidad de contar con privilegios de superadministrador.

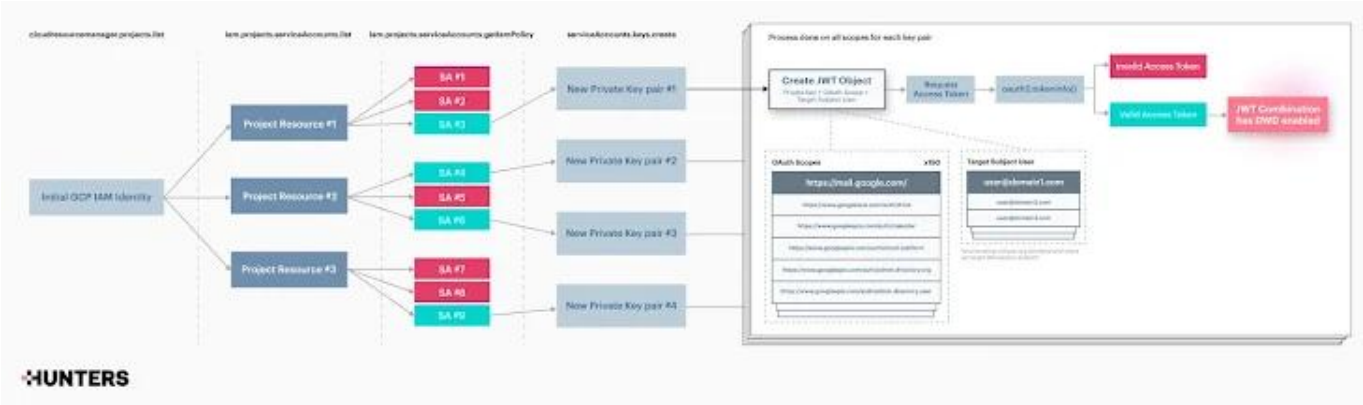
La delegación a nivel de dominio, según la descripción de Google, es una «*característica potente*» que permite a aplicaciones internas y de terceros acceder a los datos de los usuarios en el entorno de Google Workspace de una organización.

La vulnerabilidad reside en el hecho de que la configuración de la delegación de dominio está determinada por el identificador de recursos de la cuenta de servicio (OAuth ID), y no por las claves privadas específicas asociadas con el objeto de identidad de la cuenta de servicio.

En resumen, actores malintencionados con acceso menos privilegiado a un proyecto GCP objetivo podrían *«generar múltiples tokens web JSON (JWT) compuestos por diferentes alcances de OAuth, con el objetivo de identificar combinaciones exitosas de pares de claves privadas y alcances de OAuth autorizados que indiquen que la cuenta de servicio tiene la delegación a nivel de dominio habilitada».*

En otras palabras, una identidad de IAM con acceso para crear nuevas claves privadas para una cuenta de servicio relevante de GCP que cuente con permisos de delegación a nivel de

dominio puede ser utilizada para crear una nueva clave privada, la cual puede ser empleada para realizar llamadas a la API de Google Workspace en nombre de otras identidades dentro del dominio.



La explotación exitosa de esta falla podría permitir la exfiltración de datos sensibles de servicios de Google como Gmail, Drive, Calendar y otros. Hunters también ha desarrollado una prueba de concepto (PoC) que puede ser utilizado para identificar configuraciones incorrectas de DWD.

> Yonatan Khanashvili, investigador de seguridad de Hunters, advierte que «*las posibles consecuencias del uso malintencionado de la delegación a nivel de dominio son severas. En lugar de afectar solo a una identidad, como sucede con el consentimiento individual de OAuth, la explotación de DWD con delegaciones existentes puede afectar a todas las identidades dentro del dominio de Workspace*».