Investigadores de seguridad cibernética revelaron detalles de una vulnerabilidad de día cero ya parcheada en Google Cloud Platform (GCP), que podría haber permitido a los hackers de amenazas ocultar una aplicación maliciosa inamovible dentro de la cuenta de Google de una víctima.

Apodado GhostToken por la startup israelí de seguridad cibernética Astrix Security, la deficiencia afecta a todas las cuentas de Google, incluyendo las cuentas de Workspace centradas en empresas. Se descubrió y se informó a Google el 19 de junio de 2022. La empresa implementó un parche global más de nueve meses después, el 7 de abril de 2023.

> *«La vulnerabilidad permite a los atacantes obtener acceso permanente e inamovible a la cuenta de Google de la víctima al convertir una aplicación de terceros ya autorizada en una aplicación troyana maliciosa, dejando los datos personales de la víctima expuestos para siempre»,* dijo Astrix.

En pocas palabras, la vulnerabilidad hace posible que un atacante oculte su aplicación maliciosa de la página de administración de aplicaciones de la cuenta de Google de la víctima, lo que evita que los usuarios revoquen su acceso.

Esto se logra eliminando el proyecto de GCP asociado con la aplicación de OAuth autorizada, lo que hace que entre en un estado de *«eliminación pendiente».* El hacker, armado con esta capacidad, podría mostrar la aplicación no autorizada al restaurar el proyecto y usar el token de acceso para obtener los datos de la víctima y volverla invisible.

> *«En otras palabras, el atacante tiene un token 'fantasma' en la cuenta de la víctima»*, agregó Astrix.

El tipo de datos a los que se puede acceder depende de los permisos otorgados a la aplicación, de los cuales los adversarios pueden abusar para eliminar archivos de Google Drive, escribir correos electrónicos en nombre de la víctima para realizar ataques de ingeniería social, rastrear ubicaciones y filtrar datos confidenciales de Google, Calendario, Fotos y Drive.

> *«Las víctimas pueden, sin saberlo, autorizar el acceso a tales aplicaciones maliciosas al instalar una aplicación aparentemente inocente de Google Marketplace o una de las muchas herramientas de productividad disponibles en línea»,* dijo Astrix.

> *«Una vez que la aplicación maliciosa ha sido autorizada, un atacante que explote la vulnerabilidad puede eludir la función de administración de 'Aplicaciones con acceso a su cuenta' de Google, que es el único lugar donde los usuarios de Google pueden ver las aplicaciones de terceros conectadas a su cuenta»,* agregó.

El parche de Google soluciona el problema al mostrar ahora las aplicaciones que están en estado pendiente de eliminación en la página de acceso de terceros, lo que permite a los usuarios revocar el permiso otorgado a dichas aplicaciones.

El desarrollo se produce cuando Google Cloud solucionó una vulnerabilidad de escalada de privilegios en la API de inventario de activos en la nube denominada ladrón de claves de activos, que podría explotarse para el robo de claves privadas de cuentas de servicio administradas por el usuario y obtener acceso a datos valiosos. El problema, que fue descubierto por SADA a inicios de febrero, fue reparado por la compañía el 14 de marzo de 2023.