Google corrigió un error en su herramienta de comentarios incorporada en todos sus servicios, que podría ser aprovechado por un atacante para robar capturas de pantalla de documentos confidenciales de Google Docs simplemente incrustándolos en un sitio web malicioso.

La falla fue descubierta el 9 de julio por el investigador de seguridad Sreeram KL, por lo que recibió 3133.70 dólares como parte del Programa de Recompensas por Vulnerabilidad de Google.

Muchos de los productos de Google, incluyendo Google Docs, cuentan con una opción *«Enviar comentarios» o «Ayudar a que los documentos mejoren»,* que permite a los usuarios enviar comentarios junto con una opción para incluir una captura de pantalla, algo que se carga automáticamente para resaltar problemas específicos.

Pero en lugar de tener que duplicar la misma funcionalidad en todos sus servicios, la función de comentarios se implementa en el sitio web principal de Google y se integra a otros dominios a través de un elemento iframe que carga el contenido de la ventana emergente desde *«feedback.googleusercontent.com».*

Esto también indica que siempre que se incluye una captura de pantalla de la ventana de Google Docs, la representación de la imagen requiere la transmisión de los valores RGB de cada píxel al dominio principal, que luego redirige esos valores RGB al dominio de los comentarios, que finalmente construye la imagen y la envía de vuelta en forma codificado Base64.

Sreeram, sin embargo, identificó un error en la forma en que los mensajes se pasaban a «feedback.googleusercontent.com», lo que le permitía a un atacante modificar el marco a un sitio web externo arbitrario y, a su vez, robar y secuestrar capturas de pantalla de Google Docs que eran destinadas a ser subidas a los servidores de Google.

Particularmente, la vulnerabilidad se debe a la falta de un encabezado X-Frame-Options en el dominio de Google Docs, lo que hizo posible cambiar el origen de destino del mensaje y

explotar la comunicación de origen cruzado entre la página y el marco que contiene.

Aunque el ataque requiere alguna forma de interacción del usuario, es decir, hacer clic en el botón «enviar comentarios», un exploit podría aprovechar fácilmente esta debilidad para capturar la URL de la captura de pantalla cargada y exfiltrarla en un sitio malicioso.

Esto se puede lograr incrustando un archivo de Google Docs en un iFrame en un sitio web fraudulento y secuestrando el marco emergente de comentarios para redirigir el contenido a un dominio elegido por el atacante.

No proporcionar un origen de destino durante la comunicación de origen cruzado plantea problemas de seguridad, ya que revela los datos que se envían a cualquier sitio web.

> *«Siempre especifique un origen de destino exacto, no *, cuando use postMessage para enviar datos a otras ventanas. Un sitio malicioso puede cambiar la ubicación de la ventana sin su conocimiento y, por lo tanto, puede interceptar los datos enviados mediante postMessage»,* dice la documentación de Mozilla.