Microsoft reveló falla de TikTok que permitía robo de tu cuenta

Microsoft reveló una vulnerabilidad de omisión de verificación en la aplicación de Android de TikTok, lo que generó preocupaciones sobre la seguridad y la funcionalidad de la popular aplicación de redes sociales, reseña el portal TechTarget.

En una publicación de blog, Microsoft detalló la vulnerabilidad de TikTok, rastreada como CVE-2022-28799, que podría permitir a los actores de amenazas secuestrar cuentas y publicar videos privados, enviar mensajes y cargar videos en las cuentas de los usuarios. Si bien TikTok solucionó la falla y Microsoft confirmó que no observó una explotación en la naturaleza, la vulnerabilidad aumentó las preocupaciones sobre el acceso a datos privados, así como la funcionalidad del navegador en la aplicación.

Microsoft dijo que la vulnerabilidad de TikTok afectó a ambas versiones de la aplicación de Android: la compañía tiene una versión para el este y el sudeste de Asia y otra para todos los demás países, que tienen más de mil millones de descargas a través de la tienda Google Play.

En un correo electrónico a TechTarget Editorial, TikTok dijo que había «descubierto y solucionado rápidamente una vulnerabilidad en algunas versiones anteriores de la aplicación de Android».

Los investigadores describieron un ataque de prueba de concepto y riesgos adicionales en la publicación del blog de Microsoft . Para explotar la falla, un atacante enviaría un enlace de phishing al usuario objetivo, que, si se hace clic, permitiría el acceso a información confidencial. Sin embargo, Microsoft enfatizó que la explotación habría requerido que se encadenaran varios problemas, incluidos los métodos de JavaScript expuestos . Microsoft descubrió 70 métodos de JavaScript que los actores podrían haber aprovechado después de conectarse a la aplicación.

Este descubrimiento, junto con investigaciones anteriores, llevó a Microsoft a emitir una advertencia sobre los riesgos significativos asociados con las interfaces de JavaScript. Si la interfaz se ve comprometida, los atacantes pueden «ejecutar código usando la ID y los privilegios de la aplicación», según

el blog.

La vulnerabilidad de TikTok se encontró en la forma en que la aplicación de Android maneja los enlaces profundos, que Microsoft describió como «un hipervínculo especial que se vincula a un componente específico dentro de una aplicación móvil y consiste en un esquema y (generalmente) una parte de host».

Sin embargo, la falla permitió omitir la verificación del enlace profundo de la aplicación, según Microsoft, lo que permitió a los investigadores colar un enlace malicioso en WebView, un componente de Android que ejecuta el navegador en la aplicación de TikTok.

«Los atacantes podrían obligar a la aplicación a cargar una URL arbitraria en la vista web de la aplicación, lo que permitiría que la URL acceda a los puentes de JavaScript adjuntos de la vista web y otorgue funcionalidad a los atacantes», escribió Microsoft.

Fuente: TechTarget.