TikTok fue la tercera aplicación más descargada en 2019, y ahora se encuentra bajo un intenso escrutinio sobre la privacidad de los usuarios, censurando contenido políticamente controvertido y por motivos de seguridad nacional, pero además, la seguridad de los millones de usuarios ahora está en peligro.

La famosa app china para compartir videos tenía vulnerabilidades potencialmente peligrosas que podrían haber permitido a los atacantes remotos secuestrar cualquier cuenta de usuario con solo tener el número móvil de las víctimas.

En un informe compartido con The Hacker News, los investigadores de seguridad cibernética en Check Point revelaron que encadenar múltiples vulnerabilidades les permitía ejecutar remotamente código malicioso y realizar acciones no deseadas en nombre de las víctimas sin su consentimiento.

Las vulnerabilidades reportadas incluyen problemas de baja gravedad como suplantación de enlaces SMS, redirección abierta y scripting entre sitios (XSS) que al combinarse, podrían permitir que un hacker remoto realice ataques de alto impacto como:

- Eliminar videos del perfil de TikTok de las víctimas
- Subir videos no autorizados al perfil TikTok de las víctimas
- Hacer públicos los videos privados «ocultos»
- Revelar información personal guardada en la cuenta, como direcciones privadas y correos electrónicos

El ataque aprovecha un sistema de SMS inseguro que TikTok ofrece en su sitio web para permitir a los usuarios enviar un mensaje a su número de teléfono con un enlace para descargar la aplicación para compartir videos.

Según los investigadores, un atacante puede enviar un mensaje SMS a cualquier número de teléfono en nombre de TikTok con una URL de descarga modificada a una página maliciosa diseñada para ejecutar código en un dispositivo objetivo con la aplicación TikTok ya instalada.

Al combinar la dirección abierta y los problemas de secuencias de comandos entre sitios, el ataque podría permitir que los piratas informáticos ejecuten código JavaScript en nombre de las víctimas tan pronto como hagan clic en el enlace enviado por el servidor TikTok por medio de SMS, como se muestra en el video compartido por Check Point.

Esta técnica se conoce comúnmente como ataque de falsificación de solicitudes entre sitios, en el que los hackers engañan a los usuarios autenticados para que ejecuten una acción no deseada.

> *«Con la falta de un mecanismo de falsificación de solicitudes anti Cross-Site, nos dimos cuenta de que podíamos ejecutar código JavaScript y realizar acciones en nombre de la víctima, sin su consentimiento»,* dijeron los investigadores en su blog.
>
> *«Redirigir al usuario a un sitio web malicioso ejecutará un código JavaScript y hará solicitudes a TikTok con las cookies de las víctimas».*

Check Point informó responsablemente las vulnerabilidades a ByteDance, el desarrollador de TikTok, a finales de noviembre de 2019, después la empresa lanzó una versión parcheada de su aplicación móvil para proteger a sus usuarios.