Nro. Alerta:	EC-2022-087	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	06-sep-2022	VULNERABILIDAD EN TIK TOK	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de vulnerabilidad: CVE-2022-28799
Nivel de riesgo: Alto

II. ALERTA

Microsoft descubrió una vulnerabilidad de alta gravedad en la aplicación de Android TikTok, que podría haber permitido a los atacantes comprometer las cuentas de los usuarios.

Esta falla fue identificada con el CVE-2022-28799, en la cual se indica que la aplicación de Tik Tok para Android, anterior a la versión 23.7.3, permitiría a los atacantes obtener cuentas de usuarios simplemente dando clic un enlace malicioso, lo que le facilitaría el acceso a los principales controles de las cuentas afectadas.

Figura No. 1: Vulnerabilidad Tik Tok
Fuente: Una al día - Hispasec

III. INTRODUCCIÓN

Por el momento no ha habido indicios de que esta vulnerabilidad haya sido explotada a gran escala, a pesar de que las dos versiones de la aplicación de TikTok para dispositivos Android fueron afectadas, una de las versiones está destinada para el este y sureste de Asia, y la otra para el resto del mundo. Esta vulnerabilidad ha sido catalogada con alta debido a que Tik Tok tiene más de 1.500 millones de instalaciones las cuales fueron descargadas de Google Play Store.

IV. VECTOR DE ATAQUE:

Explotación de vulnerabilidad

https://www.ecucert.gob.ec @EcuCERT_EC
Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-087	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	06-sep-2022	VULNERABILIDAD EN TIK TOK	V 1.1

V. IMPACTO:

La explotación de esta vulnerabilidad podría afectar a todos los usuarios de la aplicación para el sistema operativo Android.

VI. INDICADORES DE COMPROMISO:

No aplica.

VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- Actualizar la aplicación Tik Tok.
- Activar la autenticación de dos pasos implementada por la aplicación.
- Cambiar las contraseñas de la aplicación.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *McCafferty, K. (2022, 31 agosto). Vulnerability in TikTok Android app could lead to one-click account hijacking. Microsoft Security Blog. Recuperado 6 de septiembre de 2022, de https://www.microsoft.com/security/blog/2022/08/31/vulnerability-in-tiktok-android-app-could-lead-to-one-click-account-hijacking/.*

https://www.ecucert.gob.ec @EcuCERT_EC

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec