Amazon, en diciembre de 2021, corrigió una vulnerabilidad de alta gravedad que afectaba a su aplicación Fotos para Android, y que podría haberse aprovechado para robar los tokens de acceso de un usuario.

> *«El token de acceso de Amazon se utiliza para autenticar al usuario en varias API de Amazon, algunas de las cuales contienen datos personales como el nombre completo, el correo electrónico y la dirección. Otros, como la API de Amazon Drive, permiten que un atacante tenga acceso total a los archivos del usuario»,* dijeron los investigadores de Checkmarx, Joao Morais y Pedro Umbelino.

La compañía israelí de pruebas de seguridad de aplicaciones informó el problema a Amazon el 7 de noviembre de 2021, luego de lo cual la compañía lanzó una solución el 18 de diciembre de 2021.

La fuga es el resultado de una configuración incorrecta en uno de los componentes de la aplicación llamado *«com.amazon.gallery.thor.app.activiry.ThorViewActivity»* que está definido en el archivo AndroidManifest.xml y que, al iniciarse, inicia una solicitud HTTP con un encabezado que contiene el token de acceso.

En pocas palabras, significa que una aplicación externa podría enviar una intención, un mensaje para facilitar la comunicación entre aplicaciones, para iniciar la actividad vulnerable en cuestión y redirigir la solicitud HTTP a un servidor controlado por el atacante y extraer el token de acceso.

Calificando el error como un caso de autenticación rota, la compañía de seguridad cibernética dijo que el problema podría haber permitido que las aplicaciones maliciosas instaladas en el dispositivo obtuvieran los tokens de acceso, otorgando al atacante permisos para hacer uso de las API para actividades de seguimiento.

Esto podría variar desde eliminar archivos y carpetas en Amazon Drive hasta incluso explotar el acceso para organizar un ataque de ransomware leyendo, encriptando y reescribiendo los

archivos de una víctima mientras borra su historial.

Checkmarx dijo además que la vulnerabilidad podría haber tenido un impacto más amplio debido a que las API explotadas como parte de su prueba de concepto (PoC) constituyen solo un pequeño subconjunto de todo el ecosistema de Amazon.