Investigadores de seguridad cibernética identificaron 1859 aplicaciones en Android e iOS que contienen credenciales codificadas de Amazon Web Services (AWS), lo que representa un riesgo alto de seguridad.

> *«Más de las tres cuartas partes (77%) de las aplicaciones contenían tokens de acceso de AWS válidos que permitían el acceso a servicios privados en la nube de AWS»*, dijo el equipo Threat Hunter de Symantec.

Se encontró que un poco más del 50% de las aplicaciones usaban los mismos tokens de AWS que se encuentran en otras aplicaciones mantenidas por otros desarrolladores y empresas, lo que indica una vulnerabilidad en la cadena de suministro.

> *«Los tokens de acceso de AWS podrían rastrearse hasta una biblioteca compartida, un SKD de terceros u otro componente compartido utilizado en el desarrollo de las aplicaciones»,* dijeron los investigadores.

Estas credenciales por lo general se usan para descargar los recursos apropiados necesarios para las funciones de la aplicación, así como para acceder a los archivos de configuración y autenticarse en otros servicios en la nube.

Además, el 47% de las aplicaciones identificadas contenían tokens de AWS válidos que otorgaban acceso completo a todos los archivos privados y depósitos de Amazon Simple Storage Service (S3) en la nube. Esto incluía archivos de infraestructura y copias de seguridad de datos, entre otros.

En un caso descubierto por Symantec, una empresa B2B no identificada que ofrece una intranet y una plataforma de comunicación que también proporcionaba un kit de desarrollo de software (SDK) móvil a sus clientes, tenía sus claves de infraestructura en la nube integradas en el SDK para acceder al servicio de traducción.

Esto resultó en la exposición de todos los datos privados de sus clientes, que incluían datos corporativos y registros financieros pertenecientes a más de 15,000 empresas medianas y grandes.

> *«En lugar de limitar el token de acceso codificado para su uso con el servicio de traducción en la nube, cualquier persona con el token tenía acceso total y sin restricciones a todos los servicios en la nube de AWS de la empresa B2B»*, dijeron los investigadores.

También se descubrieron cinco aplicaciones bancarias de iOS que se basan en el mismo SDK de Identidad Digital AI que contenía las credenciales de la nube, filtrando efectivamente la información de huellas dactilares de más de 300,000 usuarios.

La compañía de ciberseguridad dijo que alertó a las organizaciones sobre los problemas descubiertos en sus aplicaciones.