Investigadores en ciberseguridad han detectado serios problemas criptográficos en varias plataformas de almacenamiento en la nube con cifrado de extremo a extremo (E2EE), los cuales podrían ser explotados para filtrar información confidencial.

> *«Las vulnerabilidades varían en gravedad: en muchos casos, un servidor malicioso puede insertar archivos, alterar datos de los archivos e incluso obtener acceso directo a texto plano. Lo notable es que muchos de nuestros ataques afectan a varios proveedores de manera similar, revelando patrones comunes de fallos en diseños criptográficos independientes»*, afirmaron los investigadores de ETH Zurich, Jonas Hofmann y Kien Tuong Truong.

Los fallos descubiertos son el resultado de un análisis realizado en cinco proveedores importantes: Sync, pCloud, Icedrive, Seafile y Tresorit. Las técnicas de ataque desarrolladas dependen de un servidor malicioso controlado por un atacante, que podría ser utilizado para apuntar a los usuarios de los servicios.

A continuación, se presenta un resumen de los problemas encontrados en los sistemas de almacenamiento en la nube:

- Sync: Un servidor malicioso puede comprometer la confidencialidad de los archivos subidos, inyectar archivos y modificar su contenido.
- pCloud: Un servidor malicioso puede comprometer la confidencialidad de los archivos subidos, inyectar archivos y alterar su contenido.
- Seafile: Un servidor malicioso puede acelerar ataques de fuerza bruta contra las contraseñas de los usuarios, además de inyectar archivos y modificar su contenido.
- Icedrive: Un servidor malicioso puede comprometer la integridad de los archivos subidos, además de inyectar archivos y modificar su contenido.
- Tresorit: Un servidor malicioso puede presentar claves no auténticas al compartir archivos y alterar algunos metadatos en el almacenamiento.

Proveedores de almacenamiento en la nube

Estos ataques se agrupan en diez categorías generales que comprometen la confidencialidad, atacan los datos y metadatos de los archivos, y permiten la inyección de archivos arbitrarios:

- Falta de autenticación del material clave del usuario (Sync y pCloud).
- Uso de claves públicas no verificadas (Sync y Tresorit).
- Degradación del protocolo de cifrado (Seafile).
- Errores al compartir enlaces (Sync).
- Uso de modos de cifrado no autenticados, como CBC (Icedrive y Seafile).
- Segmentación de archivos sin autenticación (Seafile y pCloud).
- Alteración de nombres y ubicaciones de archivos (Sync, pCloud, Seafile e Icedrive).
- Manipulación de metadatos de archivos (afecta a los cinco proveedores).
- Inyección de carpetas en el almacenamiento de un usuario combinando ataques a metadatos y explotando fallos en el mecanismo de compartición (Sync).
- Inyección de archivos maliciosos en el almacenamiento de un usuario (pCloud).

> *«Muchos de nuestros ataques no son complejos, lo que significa que están al alcance de atacantes sin grandes conocimientos criptográficos. De hecho, nuestros ataques son altamente prácticos y se pueden ejecutar sin requerir muchos recursos»*, explicaron los investigadores en su informe.
>
> *«Además, aunque algunos de estos ataques no son novedosos desde una perspectiva criptográfica, subrayan que el almacenamiento en la nube con E2EE implementado en la práctica falla en aspectos básicos y, a menudo, no requiere un análisis criptográfico profundo para ser comprometido.»*

A pesar de que Icedrive ha decidido no abordar los problemas tras su divulgación en abril de 2024, Sync, Seafile y Tresorit han reconocido el informe.

Este descubrimiento llega poco más de seis meses después de que un grupo de académicos

del King's College de Londres y ETH Zurich revelara tres ataques distintos contra la función E2EE de Nextcloud, los cuales podrían comprometer la confidencialidad e integridad de los datos.

«Las vulnerabilidades facilitan que un servidor malicioso de Nextcloud acceda y manipule los datos de los usuarios», señalaron los investigadores, subrayando la importancia de tratar todas las acciones del servidor y las entradas generadas por el servidor como potencialmente adversas para solucionar estos problemas.

En junio de 2022, los investigadores de ETH Zurich también demostraron varios problemas críticos de seguridad en el servicio de almacenamiento en la nube MEGA, que podrían ser aprovechados para comprometer la confidencialidad e integridad de los datos de los usuarios.

Respuestas de las empresas

- Icedrive: Somos conscientes del informe. El estudio describe posibles ataques dentro del modelo de amenaza de «servidor comprometido», en el que un atacante obtiene control total sobre un servidor de archivos y puede modificar o eliminar datos. El informe también menciona el uso de un servidor MITM, el cual debe ser capaz de descifrar el tráfico HTTPS/SSL. Queremos tranquilizar a nuestros usuarios, ya que los datos cifrados con conocimiento cero almacenados en nuestros servidores no pueden ser descifrados sin conocer la contraseña. Si alguien obtiene control total sobre un servidor de archivos y manipula los archivos de un usuario, nuestras aplicaciones detectarán la manipulación mediante verificaciones de integridad y no descifrarán los archivos, mostrando una advertencia de error. Continuamos mejorando nuestras aplicaciones y servicios, corrigiendo problemas y agregando nuevas funciones. Revisaremos cuidadosamente nuestros métodos de cifrado y los actualizaremos conforme a los estándares de la industria.
- Sync: Nuestro equipo de seguridad se enteró de estos problemas el 11 de octubre, y desde entonces hemos tomado medidas rápidas para solucionarlos. Nos hemos puesto en contacto con el equipo de investigación para compartir hallazgos y colaborar en los

siguientes pasos. El problema de la posible fuga de datos en los enlaces ya ha sido solucionado, y estamos acelerando las correcciones para los otros problemas potenciales. Como se menciona en el informe, estas vulnerabilidades dependen de que un servidor esté comprometido. No hay evidencia de que hayan sido explotadas o que los datos hayan sido accesados. Entendemos que al usar Sync, los usuarios depositan su confianza en nosotros. Sin embargo, la promesa del cifrado de extremo a extremo es que no necesitas confiar en nadie, ni siquiera en nosotros. Este principio es clave en nuestro modelo de cifrado y central para lo que hacemos. Estamos comprometidos a resolver estos problemas.