Una nueva investigación de académicos de ETH Zurich identificó una serie de problemas de seguridad críticos en el servicio de almacenamiento en la nube de MEGA que podrían aprovecharse para evitar la confidencialidad e integridad de los datos del usuario.

En un artículo titulado «MEGA: Maleable Encryption Goes Awry«, los investigadores señalan cómo el sistema de MEGA no protege a sus usuarios contra un servidor malicioso, lo que permite que un atacante comprometa por completo la privacidad de los archivos cargados.

> *«Además, la integridad de los datos del usuario se daña en la medida en que un atacante puede insertar archivos maliciosos de su elección que pasan todas las verificaciones de autenticidad del cliente»*, dijeron Matilda Backendal, Miro Haller y Kenneth G. Paterson, de ETH Zurich.

MEGA, que se anuncia a sí misma como *«la compañía de privacidad»* y asegura proporcionar almacenamiento en la nube encriptado de extremo a extremo controlado por el usuario, tiene más de 10 millones de usuarios activos diarios, con más de 122 mil millones de archivos cargados en la plataforma hasta ahora.

La principal de las fallas consta de un ataque de recuperación de clave RSA que hace posible que MEGA (maliciosamente) o un adversario del estado-nación que controla su infraestructura API recupere la clave privada RSA de un usuario manipulando 512 intentos de inicio de sesión y descifrando el contenido almacenado.

> *«Una vez que una cuenta objetivo había realizado suficientes inicios de sesión exitosos, las carpetas compartidas entrantes, los archivos MEGAdrop y los chats podrían haber sido descifrados. Los archivos en la unidad de la nube podrían haberse descifrado sucesivamente durante los inicios de sesión posteriores»,* dijo Mathias Ortmann, arquitecto jefe de MEGA.

La clave RSA recuperada se puede ampliar para dar paso a otros cuatro ataques:

- Plaintext Recovery Attack: Permite a MEGA descifrar claves de nodo, una clave de cifrado asociada con cada archivo cargado y cifrada con la clave maestra de un usuario, y usarlas para descifrar todas las comunicaciones y archivos del usuario.
- Framing Attack: MEGA puede insertar archivos arbitrarios en el almacenamiento de archivos del usuario que son indistinguibles de los cargados de forma genuina.
- Integrity Attack: Una variante menos sigilosa del Framing Attack que puede explotarse para falsificar un archivo a nombre de la víctima y colocarlo en el almacenamiento en la nube del objetivo.
- Guess-and-Purge (GAP) Bleichenbacher Attack: Una variante del ataque de texto cifrado elegido adaptativo ideado por el criptógrafo suizo Daniel Bleichenbacher en 1998 que podría explotarse para descifrar textos de cifrados RSA.

> *«Cada usuario tiene una clave RSA pública utilizada por otros usuarios o MEGA para cifrar datos para el propietario, y una clave privada utilizada por el propio usuario para descifrar datos compartidos con ellos. Con este ataque, MEGA puede descifrar estos textos cifrados RSA, aunque requiere una cantidad poco práctica de intentos de inicio de sesión»,* explicaron los investigadores.

En otras palabras, los ataques podrían ser armados por MEGA o cualquier entidad que controle su infraestructura central para cargar archivos similares y descifrar todos los archivos y carpetas que pertenecen o se comparten con la víctima, así como los mensajes de chat intercambiados.

Las deficiencias son graves ya que socavan las supuestas garantías de seguridad de MEGA, lo que llevó a la compañía a publicar actualizaciones para abordar los primeros tres de los cinco problemas. Se espera que la cuarta vulnerabilidad relacionada con la violación de la integridad se aborde en una próxima versión.

En cuanto al ataque estilo Bleichenbacher contra el mecanismo de encriptación RSA de

MEGA, la compañía dijo que el ataque es *«difícil de realizar en la práctica, ya que requeriría aproximadamente 122,000 interacciones de clientes en promedio»* y que eliminaría el código heredado de todos sus clientes.

MEGA enfatizó además que no tiene conocimiento de ninguna cuenta de usuario que pueda haber sido comprometida por los métodos de ataque ya mencionados.

> *«Las vulnerabilidades informadas habrían requerido que MEGA se convirtiera en un mal actor contra algunos de sus usuarios, o de lo contrario solo podrían explotarse si otra parte comprometiera los servidores API de MEGA o las conexiones TLS sin ser notado»,* dijo Ortmann.

> *«Los ataques [...] surgen de interacciones inesperadas entre componentes aparentemente independientes de la arquitectura criptográfica de MEGA. Insinúan la dificultad de mantener sistemas a gran escala que emplean criptografía, especialmente cuando el sistema tiene un conjunto de funciones en evolución y se implementa en múltiples plataformas»,* dijeron los investigadores.

> *«Los ataques presentados aquí muestran que es posible que una parte motivada encuentre y explote vulnerabilidades en arquitecturas criptográficas del mundo real, con resultados devastadores para la seguridad. Es concebible que los sistemas en esta categoría atraigan a adversarios que estén dispuestos a invertir recursos significativos para comprometer el propio servicio, aumentando la plausibilidad de los ataques de alta complejidad».*