Un investigador de seguridad cibernética reveló hoy los detalles de una vulnerabilidad en el navegador web Safari, que se podría permitir que un atacante robe archivos de los dispositivos de los usuarios.

El error fue descubierto por Pawel Wylecial, cofundador de la compañía de seguridad polaca REDTEAM.PL.

Wylecial informó el error a Apple a inicios de abril, pero el investigador decidió hacer públicos sus hallazgos este lunes después de que la compañía de la manzana retrasara la corrección del error por casi un año, hasta la primavera de 2021.

En una publicación, Wylecial dijo que la vulnerabilidad reside en la implementación de Safari de la API Web Share, un nuevo estándar web que introdujo una API entre navegadores para compartir texto, enlaces, archivos y otro contenido.

El investigador de seguridad dice que Safari, tanto para iOS como para MacOS, admite compartir archivos que están almacenados en el disco duro local del usuario, a través del esquema file://URI.

Esto es un gran problema de privacidad, ya que podría permitir situaciones en las que sitios web maliciosos inviten a los usuarios a compartir un artículo por correo electrónico con sus contactos, pero también extrayendo o filtrando en secreto un archivo en el dispositivo.

El siguiente video de demostración muestra cómo se puede explotar el error para obtener información de /etc/passwd o el historial de navegador de bases de datos.

Wylecial describió el error como *«no muy grave»*, ya que se necesita la interacción del usuario y la ingeniería social compleja para engañar a los usuarios para que filtren archivos locales, sin embargo, también admitió que es muy fácil para los atacantes *«hacer que el archivo compartido sea invisible para el usuario».*

Pero otro problema es la forma en que Apple manejó el informe del error. Aparte de no poder

tener listo el parche después de más de cuatro meses, también intentó retrasar al investigador para que no publicara sus hallazgos hasta la siguiente primavera, casi un año completo desde el informe de error original y más allá del plazo estándar de divulgación de 90 días.

Apple es constantemente acusada por retrasar la divulgación de errores a propósito y tratar de silenciar a los investigadores, a pesar de tener un programa dedicado de recompensas de errores.