Se han revelado detalles sobre una vulnerabilidad de seguridad de gravedad considerable en la aplicación Shortcuts de Apple, la cual ha sido corregida y que podría posibilitar que un atajo acceda a información delicada en el dispositivo sin el consentimiento del usuario.

La vulnerabilidad, identificada como CVE-2024-23204 (puntuación CVSS: 7.5), fue abordada por Apple el 22 de enero de 2024, con la liberación de iOS 17.3, iPadOS 17.3, macOS Sonoma 14.3 y watchOS 10.3.

> *«Un atajo podría tener la capacidad de utilizar datos sensibles con ciertas acciones sin requerir la autorización del usuario»*, afirmó el fabricante del iPhone en un comunicado, indicando que se solucionó mediante *«verificaciones de permisos adicionales»*.

Apple Shortcuts es una aplicación de secuencias de comandos que permite a los usuarios diseñar flujos de trabajo personalizados (también conocidos como macros) para ejecutar tareas específicas en sus dispositivos. Viene preinstalado por defecto en los sistemas operativos iOS, iPadOS, macOS y watchOS.

Jubaer Alnazi Jabin, investigador de seguridad de Bitdefender, quien descubrió y reportó el fallo en Shortcuts, sostuvo que podría ser utilizado para crear un atajo malicioso que evite las políticas de Transparencia, Consentimiento y Control (TCC).

TCC es un marco de seguridad de Apple diseñado para salvaguardar los datos del usuario contra accesos no autorizados sin solicitar los permisos adecuados en primera instancia.

En particular, la falla radica en una acción de atajo denominada *«Expandir URL»,* que es capaz de desarrollar y depurar URLs que han sido acortadas mediante un servicio de acortamiento de URL como t.co o bit.ly, al tiempo que elimina parámetros de seguimiento UTM.

> *«Al aprovechar esta funcionalidad, se hizo posible transmitir los datos codificados en Base64 de una foto a un sitio web malintencionado»,* explicó Alnazi Jabin.
>
> *«El método implica seleccionar cualquier dato delicado (fotos, contactos, archivos y datos del portapapeles) dentro de Shortcuts, importarlo, convertirlo usando la opción de codificación base64 y, finalmente, enviarlo al servidor malintencionado».*

Los datos extraídos son entonces capturados y guardados como una imagen en el extremo del atacante mediante una aplicación Flask, allanando el camino para una posterior explotación.

> *«Los atajos pueden ser exportados y compartidos entre usuarios, una práctica común en la comunidad de Shortcuts. Este mecanismo de intercambio amplía el alcance potencial de la vulnerabilidad, ya que los usuarios importan atajos que podrían aprovechar CVE-2024-23204 sin estar al tanto»,* indicó el investigador.