Una nueva investigación descubrió vulnerabilidades de privacidad en el protocolo de intercambio de archivos inalámbrico de Apple, que podrían resultar en la exposición de la información de contacto de un usuario, como direcciones de correo electrónico y números de teléfono.

> *«Como atacante, es posible conocer los números de teléfono y las direcciones de correo electrónico de los usuarios de AirDrop, incluso como un completo extraño. Todo lo que necesitan es un dispositivo con capacidad WiFi y proximidad física a un objetivo que inicie el proceso de descubrimiento abriendo el panel para compartir en un dispositivo iOS o macOS»,* dijo un equipo de académicos de la Universidad Técnica de Darmstadt, Alemania.

AirDrop es un servicio ad hoc patentado presente en los sistemas operativos iOS y macOS de Apple, que permite a los usuarios transferir archivos entre dispositivos mediante la comunicación inalámbrica de corto alcance.

Aunque esta función muestra solo los dispositivos receptores que están en las listas de contactos de los usuarios mediante un mecanismo de autenticación que compara el número de teléfono y la dirección de correo electrónico de un individuo con las entradas en la libreta de direcciones del otro usuario, la nueva deficiencia anula dichas protecciones con la ayuda de un dispositivo WiFi capaz, simplemente por estar en estrecha proximidad física a un objetivo.

> *«Cuando se intenta una conexión AirDrop entre un remitente y un receptor, el remitente transmite por aire un mensaje que contiene un hash, o huella digital, de la dirección de correo electrónico o número de teléfono de su usuario como parte de un apretón de manos de autenticación. En respuesta, si se reconoce al remitente, el receptor transmite su hash»,* explicaron los investigadores.

Según los investigadores, el núcleo del problema tiene su origen en el uso de funciones hash por parte de Apple para enmascarar los identificadores de contacto intercambiados, es decir, números de teléfono y direcciones de correo electrónico, durante el proceso de descubrimiento.

Un receptor malintencionado no solo puede recopilar los identificadores de contacto con hash y descifrarlos *«en milisegundos»* utilizando técnicas como ataques de fuerza bruta, sino que un remitente malintencionado también puede aprender todos los identificadores de contacto con hash, incluido el número de teléfono del receptor, sin necesidad de previo conocimiento del receptor.

En un escenario hipotético de ataque, un gerente puede abrir un menú para compartir una hoja de Apple que podría usarse para obtener el número de teléfono o la dirección de correo electrónico de otros empleados que tienen los datos de contacto del gerente almacenados en sus libretas de direcciones.

Los investigadores dijeron que notificaron en privado a Apple sobre el problema ya en mayo de 2019, y una vez más en octubre de 2020 luego de desarrollar una solución llamada «*PrivateDrop*» para corregir el diseño defectuoso en AirDrop.

> *«PrivateDrop se basa en protocolos de intersección de conjuntos privados criptográficos optimizados que pueden realizar de forma segura el proceso de descubrimiento de contactos entre dos usuarios sin intercambiar valores hash vulnerables»*, dijeron los investigadores.

Pero debido a que Apple aún no indica sus planes para solucionar la filtración de privacidad, los usuarios de más de 1500 millones de dispositivos Apple son vulnerables a tales ataques.

> *«Los usuarios solo pueden protegerse si deshabilitan el descubrimiento de AirDrop en la configuración del sistema y se abstienen de abrir el menú para compartir»,*

> dijeron los investigadores.

Los hallazgos son los últimos de una serie de estudios realizados por investigadores de TU, que han desmontado el ecosistema inalámbrico de Apple a lo largo de los años con el objetivo de identificar problemas de seguridad y privacidad.

En mayo de 2019, los investigadores revelaron vulnerabilidades en el protocolo de red de malla patentado Wireless Direct Link (AWDL) de Apple, que permitía a los atacantes rastrear usuarios, bloquear dispositivos e incluso interceptar archivos transferidos entre dispositivos a través de ataques man-in-the-middle (MitM).

Después, a inicios del mes pasado, se descubrieron dos fallas distintas de diseño e implementación en la función Find My de Apple, que podrían conducir a un ataque de correlación de ubicación y acceso no autorizado al historial de ubicaciones de los últimos siete días, desanonimizando a los usuarios.