Las últimas investigaciones demostraron un nuevo exploit que permite cargar datos arbitrarios desde dispositivos que no están conectados a Internet simplemente enviando transmisiones *«Find My Bluetooth»* a dispositivos Apple cercanos.

> *«Es posible cargar datos arbitrarios desde dispositivos no conectados a Internet enviando transmisiones de Find My [Bluetooth Low Energy] a dispositivos Apple cercanos que luego cargan los datos por ti»,* dijo Fabian Bräunlein, investigador de Positive Security.
>
> *«Al ser inherente al diseño centrado en la privacidad y la seguridad del sistema Find My Offline Finding, parece poco probable que este uso indebido pueda prevenirse completamente»,* agregó.

El estudio se basa en un estudio anterior de TU Darmstadt publicado en marzo de 2021, que reveló dos fallas distintas de diseño e implementación en el sistema de seguimiento de ubicación de Bluetooth de colaboración colectiva de Apple que podrían conducir a un ataque de correlación de ubicación y acceso no autorizado al historial de ubicación de un usuario de los últimos siete días.

Esta investigación se agrandó con el lanzamiento de un marco llamado OpenHaystack que está diseñado para permitir que cualquier usuario cree un *«AirTag»*, lo que permite a las personas rastrear dispositivos Bluetooth personales a través de la red Find My de Apple.

Sin embargo, la ingeniería inversa del sistema de búsqueda fuera de línea Find My de Apple, también dejó la puerta abierta a la posibilidad de que el protocolo pudiera emularse para cargar datos arbitrarios a Internet transmitiendo la información a través de balizas Bluetooth que serían recogidas por dispositivos Apple en contacto físico cercano, y luego retransmitir los datos cifrados a los servidores de Apple, desde donde una aplicación macOS puede recuperar, decodificar y mostrar los datos cargados.

Uno de los aspectos centrales de Find My es su esquema de clave rotativa que consiste en un par de claves públicas-privadas que se cambian de forma determinista cada 15 minutos, con la clave pública enviada dentro del paquete de publicidad de Bluetooth Low Energy.

Por lo tanto, cuando los dispositivos Apple cercanos, como MacBooks, iPhones y iPads, reciben la transmisión, obtienen su propia ubicación y luego encriptan la ubicación usando la clave pública antes mencionada, antes de enviar el informe de ubicación encriptado a iCloud junto con un hash de la clave pública. En el paso final, el propietario del dispositivo perdido puede usar un segundo dispositivo Apple que haya iniciado sesión con el mismo ID de Apple para acceder a la ubicación aproximada.

Las protecciones de cifrado significan que Apple no solo sabe qué claves públicas pertenecen a un dispositivo perdido específico o AirTag, sino que tampoco sabe qué informes de ubicación están destinados a un usuario específico, de ahí el requisito de ID de Apple anterior.

> *«La seguridad radica únicamente en el cifrado de los informes de ubicación: la ubicación sólo se puede descifrar con la clave privada correcta, que es inviable a la fuerza bruta y solo se almacena en el dispositivo propietario emparejado»,* dijo Bräunlein.

Por lo tanto, la idea es aprovechar la brecha codificando un mensaje en las cargas útiles de transmisión y luego obteniéndolos en el otro extremo utilizando un componente de recuperación de datos basado en OpenHaystack, que descifra y extrae la información transmitida desde el dispositivo remitente, como un microcontrolador.

> *«Al enviar los datos, se codifican en las claves públicas que son transmitidas por el*

> *microcontrolador. Los dispositivos Apple cercanos recogerán esas transmisiones y reenviarán los datos a un backend de Apple como parte de sus informes de ubicación. Esos informes pueden ser recuperados más tarde por cualquier dispositivo Mac para decodificar los datos enviados»,* dijo Bräunlein.

Aunque las implicaciones maliciosas en el mundo real de un exploit de este tipo pueden parecer discutibles, también es difícil para Apple defenderse de un ataque de este tipo debido a la naturaleza encriptada de un extremo a otro de la red Find My.

Para contrarrestar estos usos no deseados, el investigador sugiere fortalecer el sistema de dos formas posibles, incluyendo una autenticación del anuncio BLE y la aplicación de límites de frecuencia en las recuperaciones de informes en el lugar almacenando los valores hash en caché y asegurándose de que los únicos *«16 nuevos ID de clave se consultan cada 15 minutos»*. Cabe mencionar que existe un límite de 16 AirTags por ID de Apple.

> *«En el mundo de las redes de alta seguridad, donde la combinación de láseres y escáneres parece ser una técnica notable para cerrar la brecha de aire, los dispositivos Apple del visitante también podrían convertirse en intermediarios factibles para exfiltrar datos de ciertos sistemas con brecha de aire o habitaciones enjauladas de Faraday»*, dijo Bräunlein.