Investigadores de seguridad cibernética revelaron este jueves dos vulnerabilidades distintas de diseño e implementación en el sistema de seguimiento de ubicación de Bluetooth de colaboración colectiva de Apple que pueden 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.

Las revelaciones son consecuencia de una revisión exhaustiva realizada por el proyecto Open Wireless Link (OWL), un equipo de investigadores del Laboratorio de Redes Móviles Seguras de la Universidad Técnica de Darmstadt, Alemania, que históricamente han desarmado el ecosistema inalámbrico de Apple con el objetivo de identificar problemas de seguridad y privacidad.

En respuesta a las divulgaciones del 2 de julio de 2020, se dice que Apple ha abordado parcialmente los problemas, según los investigadores, que utilizaron sus propios datos para el estudio citando las implicaciones de privacidad del análisis.

Los dispositivos de Apple cuentan con una función llamada Find My, que facilita a los usuarios localizar otros dispositivos Apple, incluyendo iPhone, iPad, iPod Touch, Apple Watch, Mac o AirPods.

Con el próximo iOS 14.5, se espera que la compañía agregue soporte para dispositivos de rastreo Bluetooth, llamados AirTags, que se pueden adjuntar a elementos como llaves y billeteras, que a su vez se puede usar con fines de rastreo desde la aplicación Find My.

La tecnología Find My, llamada búsqueda fuera de línea, fue introducida en 2019. La función de seguimiento de ubicación transmite señales de Bluetooth Low Energy (BLE) desde dispositivos Apple, lo que permite que otros dispositivos Apple en las proximidades transmitan su ubicación a los servidores de Apple.

Esto significa que, la carga fuera de línea convierte cada dispositivo móvil en una baliza de transmisión diseñada explícitamente para ocultar sus movimientos al aprovechar un mecanismo de seguimiento de ubicación de colaboración colectiva que es cifrado de extremo

a extremo y anónimo, por lo que ningún tercero, incluido Apple, puede descifrar esas ubicaciones y crear un historial del paradero de cada usuario.

Esto se realiza mediante un esquema de clave rotativa, específicamente un par de claves público-privadas que son generadas por cada dispositivo, que emite las señales de Bluetooth codificando la clave pública junto con él. Esta información clave se sincroniza posteriormente a través de iCloud con todos los demás dispositivos Apple vinculados al mismo usuario.

Un iPhone o iPad cercano (sin conexión con el dispositivo fuera de línea original) que percibe este mensaje verifica su propia ubicación, luego encripta la información usando la clave pública antes mencionada antes de enviarla a la nube junto con un hash de la clave pública.

Finalmente, Apple envía la ubicación encriptada del dispositivo perdido a un segundo dispositivo Apple que inició sesión con el mismo ID de Apple, desde donde el propietario puede usar la aplicación Find My para descifrar los informes usando la clave privada correspondiente y recuperar la última ubicación conocida, con el dispositivo complementario cargando el mismo hash de la clave pública para encontrar una coincidencia en los servidores de Apple.

Debido a que el enfoque sigue una configuración de cifrado de clave pública (PKE), incluso Apple no puede descifrar la ubicación porque no está en posesión de la clave privada. Si bien la compañía no ha revelado explícitamente la frecuencia con la que gira la clave, la arquitectura de par de claves cambiantes dificulta que las partes malintencionadas aprovechen las balizas de Bluetooth para rastrear los movimientos de los usuarios.

Pero los investigadores de OWL dijeron que el diseño permite a Apple, en lugar de ser el proveedor de servicios, correlacionar las ubicaciones de diferentes propietarios si sus ubicaciones son informadas por los mismos dispositivos de búsqueda, lo que permite a Apple construir lo que ellos llaman un gráfico social.

> *«Los organismos encargados de hacer cumplir la ley podrían explotar este problema para desanonimizar a los participantes de manifestaciones incluso cuando los participantes ponen sus teléfonos en modo de vuelo. Las aplicaciones macOS maliciosas pueden recuperar y descifrar los informes de ubicación de los últimos siete días para todos sus usuarios y para todos sus dispositivos, ya que las claves de anuncios rodantes en caché se almacenan en el sistema de archivos en texto sin cifrar»,* dijeron los investigadores.

La vulnerabilidad macOS Catalina (CVE-2020-9986) podría permitir que un atacante acceda a las claves de descifrado, utilizándolas para descargar y descifrar los informes de ubicación enviados por la red Find My, y en última instancia, localizar e identificar a sus víctimas con alta precisión. Apple corrigió la vulnerabilidad en noviembre de 2020 con *«restricciones de acceso mejoradas».*

Un segundo resultado de la investigación es una aplicación que está diseñada para permitir que cualquier usuario cree un «AirTag». Llamado OpenHaystack, el marco permite rastrear dispositivos Bluetooth personales a través de la red masiva Find My de Apple, lo que permite a los usuarios crear sus propias etiquetas de rastreo que se pueden agregar a objetos físicos o integrar en otros dispositivos con capacidad Bluetooth.

Esta no es la primera vez que los investigadores de Open Wireless Link (OWL) han descubierto fallas en los protocolos de código cerrado de Apple mediante ingeniería inversa.