El primer análisis de seguridad de su tipo de la función Find My de iOS, identificó una nueva superficie de ataque que hace posible manipular el firmware y cargar malware en un chip Bluetooth que se ejecuta mientras el iPhone está *«apagado».*

El mecanismo aprovecha el hecho de que los chips inalámbricos relacionados con Bluetooth, la comunicación de campo cercano (NFC) y la banda ultraancha (UWB) siguen funcionando mientras iOS se apaga al entrar en un modo de bajo consumo (LPM) de *«reserva de energía».*

Aunque esto se hace para habilitar funciones como Find My y facilitar las transacciones de Express Card, los tres chips inalámbricos tienen acceso directo al elemento seguro, dijeron los académicos del Laboratorio de Redes Móviles Seguras (SEEMOO) de la Universidad Técnica de Darmstadt.

> *«Los chips Bluetooth y UWB están conectados al elemento seguro (SE) en el chip NFC, almacenando secretos que deberían estar disponibles en LPM»*, dijeron los investigadores.

> *«Debido a que el soporte LPM está implementado en el hardware, no se puede eliminar cambiando los componentes del software. Como resultado, en los iPhones modernos, ya no se puede confiar en que los chips inalámbricos se apaguen después del apagado. Esto plantea un nuevo modelo de amenaza».*

Los hallazgos se presentarán en la Conferencia ACM sobre seguridad y privacidad en redes inalámbricas y móviles (WiSec 2022) esta semana.

Las características de LPM, recientemente introducidas en el año pasado con iOS 15, hacen posible rastrear dispositivos perdidos utilizando la red Find My, incluso cuando se han quedado sin batería o se han apagado. Los dispositivos actuales con soporte de banda ultraancha incluyen iPhone 11, iPhone 12 y iPhone 13.

Un mensaje que se muestra cuando se apagan los iPhone dice lo siguiente:

> *«El iPhone permanece localizable después del apagado. Find My lo ayuda a ubicar este iPhone cuando se pierde o se lo roban, incluso cuando está en modo de reserva de energía o cuando está apagado».*

Llamando a la implementación actual de LPM *«opaca»,* los investigadores no solo observaron fallas al inicializar los anuncios Find My durante el apagado, contradiciendo efectivamente el mensaje mencionado, además de encontrar que el firmware de Bluetooth no está firmado ni encriptado.

Al aprovechar esta laguna, un adversario con acceso privilegiado puede crear malware que puede ejecutarse en un chip Bluetooth de iPhone incluso cuando está apagado.

Sin embargo, para que ocurra dicho compromiso de firmware, el atacante debe poder comunicarse con el firmware a través del sistema operativo, modificar la imagen del firmware u obtener la ejecución del código en un chip habilitado para LPM por aire al explotar vulnerabilidades como BrakTooth.

En otras palabras, la idea es alterar el hilo de la aplicación LPM para incrustar malware, como aquellos que podrían alertar al actor malicioso de las transmisiones Find My Bluetooth de una víctima, lo que permite al atacante mantener un control remoto del objetivo.

> *«En lugar de cambiar la funcionalidad existente, también podrían agregar características completamente nuevas»*, dijeron los investigadores de SEEMOO.

Dado que las funciones relacionadas con LPM adoptan un enfoque más sigiloso para realizar los casos de uso previstos, SEEMOO pidió a Apple que incluyera un interruptor basado en hardware para desconectar la batería a fin de aliviar cualquier problema de vigilancia que pudiera surgir de los ataques a nivel de firmware.

> *«Debido a que la compatibilidad con LPM se basa en el hardware del iPhone, no se puede eliminar con las actualizaciones del sistema. Por lo tanto, tiene un efecto duradero en el modelo general de seguridad de iOS»,* dijeron los investigadores.

> *«El diseño de las características de LPM parece estar impulsado principalmente por la funcionalidad, sin tener en cuenta las amenazas fuera de las aplicaciones previstas. Find My después de apagar convierte los iPhone apagados en dispositivos de seguimiento por diseño, y la implementación dentro del firmware de Bluetooth no está protegida contra la manipulación».*