Miles de millones de dispositivos como teléfonos inteligentes, tabletas electrónicas, computadoras y dispositivos IoT, están utilizando pilas de software Bluetooth que son vulnerables a una nueva vulnerabilidad revelada durante el verano.

BLESA (Bluetooth Low Energy Spoofing Attack), es el nombre que se le dio a la vulnerabilidad, que afecta a los dispositivos que ejecutan el protocolo Bluetooth Low Energy (BLE).

BLE es una versión más liviana del estándar Bluetooth original, pero está diseñada para conservar la energía de la batería mientras mantiene activas las conexiones Bluetooth el mayor tiempo posible.

Debido a sus características de ahorro de batería, BLE se ha adoptado masivamente durante la última década, convirtiéndose en una tecnología casi omnipresente en casi todos los dispositivos que funcionan con baterías.

Como resultado de la amplia adopción, los investigadores y académicos de seguridad también investigaron repetidamente BLE en busca de fallas de seguridad a lo largo de los años, encontrando varias veces problemas importantes.

Sin embargo, la gran mayoría de las investigaciones anteriores sobre los problemas de seguridad en BLE se centraron casi de forma exclusiva en el proceso de emparejamiento, ignorando de este modo las grandes partes del protocolo BLE.

En un proyecto de investigación de la Universidad de Purdue, un equipo de siete académicos investigó una sección del protocolo BLE que juega un papel crucial en las operaciones BLE diarias, pero que rara vez se ha analizado en busca de problemas de seguridad.

El trabajo se centró en el proceso de *«reconexión»*. Esta operación tiene lugar después de que dos dispositivos BLE (cliente y servidor) se hayan autenticado durante la operación de emparejamiento.

Las reconexiones tienen lugar cuando los dispositivos Bluetooth se mueven fuera del alcance y luego vuelven a estar dentro del alcance más tarde. Normalmente, al volver a conectarse, los dos dispositivos BLE deben verificar las claves criptográficas del otro negociando durante el proceso de emparejamiento, y volver a conectarse y seguir intercambiando datos a través de BLE.

Pero el equipo de investigación de Purdue dijo que descubrió que la especificación oficial de BLE no contenía un lenguaje lo suficientemente fuerte para describir el proceso de reconexión. Como resultado, dos problemas sistémicos se abrieron camino en las implementaciones de software BLE a lo largo de la cadena de suministro:

- La implementación durante la reconexión del dispositivo es opcional en lugar de obligatoria.
- La autenticación se puede eludir potencialmente si el dispositivo del usuario no logra hacer cumplir el dispositivo IoT para autenticar los datos comunicados.

Estos dos problemas pueden permitir un ataque BLESA, en el que un atacante cercano omite las verificaciones de reconexión y envía datos falsificados a un dispositivo BLE con información incorrecta, e induce a los operadores humanos y los procesos automatizados a tomar decisiones erróneas.

Sin embargo, el problema no ha aparecido en todas las implementaciones de BLE en el mundo real.

Los investigadores de Purdue dijeron que analizaron múltiples pilas de software que se han utilizado para respaldar las comunicaciones BLE en distintos sistemas operativos.

También descubrieron que BlueZ (dispositivos IoT basados en Linux), Fluoride (Android) y la pila BLE de iOS, eran vulnerables a los ataques BLESA, mientras que la pila BLE en los dispositivos Windows era inmune.

> *«A partir de junio de 2020, aunque Apple asignó el CVE-2020-9770 a la vulnerablidad y la solucionó, la implementación de Android BLE en nuestro dispositivo probado sigue siendo vulnerable»*, dijeron los investigadores el mes pasado.

En cuanto a los dispositivos IoT basados en Linux, el equipo de desarrollo de BlueZ dijo que desaprobaría la parte de su código que abre los dispositivos a los ataques de BLESA, y en su lugar, usará código que implemente los procedimientos de reconexión BLE adecuados, inmune a BLESA.

Lamentablemente, al igual que con todos los errores de Bluetooth anteriores, parchear todos los dispositivos vulnerables sería una tarea demasiado complicada para los administradores de sistemas, y algunos dispositivos no podrían ser parcheables.

Algunos equipos de IoT con recursos limitados que se han vendido durante la última década y que ya se han implementado en el campo actualmente, no cuentan con un mecanismo de actualización incorporado, lo que significa que esos dispositivos permanecerán sin parches permanentemente.

Los atacantes podrían utilizar errores de denegación de servicio para hacer que las conexiones Bluetooth se desconecten y activen una operación de reconexión bajo demanda, y luego ejecuten un ataque BLESA. Es imposible proteger los dispositivos BLE contra desconexiones y caídas de señal.

Los detalles adicionales sobre el ataque BLESA están disponibles en el documento «*BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy*«.

El documento fue presentado en la conferencia USENIX WOOT 2020 en agosto. Se puede ver una grabación de la presentación en el siguiente video.