Un equipo de investigadores de seguridad cibernética reveló este fin de semana informes sobre 12 vulnerabilidades potencialmente graves, denominadas de forma colectiva como «SweynTooth», que afectan a millones de dispositivos inteligentes inalámbricos habilitados para Bluetooth en todo el mundo.

Todas las vulnerabilidades de SweynTooth residen básicamente en la forma en que los kits de desarrollo de software (SDK) utilizados por múltiples sistemas en un chip (SoC) implementaron la tecnología de comunicación inalámbrica Bluetooth Low Energy (BLE), que alimenta al menos 480 productos diferentes de distintos proveedores, incluyendo Samsung, FitBit y Xiaomi.

Según los investigadores, los hackers en proximidad física cercana a dispositivos vulnerables pueden abusar de la vulnerabilidad para activar remotamente puntos muertos, bloqueos e incluso eludir la seguridad de los protocolos BLE, lo que les permite acceso de lectura o escritura arbitrario a las funciones del dispositivo que de otra forma, solo se les permitiría Accedido por un usuario autorizado.

> *«A partir de hoy, las vulnerabilidades SweynTooth se encuentran en los SDK BLE vendidos por los principales proveedores de SoC, como Texas Instruments, NXP, Cypress, Dialog Semiconductors, Microchip, STMicroelectronics y Telink Semiconductor»,* dijeron los investigadores de la Universidad de Tecnología y Diseño de Singapur.

Las 12 vulnerabilidades se describen brevemente a continuación:

- Desbordamiento de la longitud de la capa de enlace (CVE-2019-16336, CVE-2019-17519): Permiten a los atacantes en el rango de radio, activar un desbordamiento del búfer al manipular el campo de longitud LL, lo que conduce principalmente a ataques de denegación de servicio.
- Punto muerto de LLID de capa de enlace (CVE-2019-17061, CVE-2019-17060): Activan el estado de punto muerto cuando un dispositivo recibe un paquete con el campo LLID

borrado.

- L2CAP truncado (CVE-2019-17517): Esta falla se debe a la falta de verificaciones al procesar un paquete L2CAP, lo que provoca una denegación de servicio y un bloqueo del dispositivo.
- Desbordamiento de longitud silenciosa (CVE-2019-17518): Se produce un desbordamiento de búfer cuando se envía una determinada carga útil de paquete con una longitud LL superior a la esperada, el periférico se bloquea.
- Solicitud de conexión no válida (CVE-2019-19195): Cuando los dispositivos no manejan correctamente algunos parámetros de conexión mientras la central intenta una conexión al periférico, podrían conducir al estado de bloqueo.
- Accidente de clave pública inesperado (CVE-2019-17520): Este error está presente en la implementación del procedimiento de emparejamiento heredado, que se maneja mediante la implementación del Protocolo de Administrador Seguro (SMP), y puede usarse para realizar DoS y posiblemente reiniciar productos.
- Bloqueo secuencial de ATT (CVE-2019-19192): Esta falla permite a los atacantes bloquear el periférico enviando solo dos paquetes de solicitud ATT consecutivos en cada evento de conexión.
- Fragmento L2CAP no válido (CVE-2019-19195): El manejo incorrecto del tamaño de PDU de los paquetes puede conducir a un comportamiento de punto muerto.
- Desbordamiento del tamaño de la clave (CVE-2019-19196): Este desbordamiento en el problema de memoria del dispositivo es una combinación de múltiples errores encontrados durante el procedimiento de emparejamiento de dispositivos, lo que resulta en un bloqueo.
- Instalación cero LTK (CVE-2019-19194): Esta vulnerabilidad crítica es una variación de uno de los desbordamientos de tamaño de clave. Afecta a todos los productos que utilizan la implementación Telink SMP con soporte para conexión segura habilitada.

El informe detallado especifica que los productos afectados incluyen productos electrónicos de consumo, dispositivos domésticos inteligentes, dispositivos portátiles, y también se están utilizando en la industria de la logística y atención médica, cuyo mal funcionamiento puede conducir a situaciones peligrosas.

> *«Los dispositivos más críticos que podrían verse gravemente afectados por SweynTooth son los productos médicos. Los laboratorios VivaCheck, que fabrican medidores de glucosa en sangre, tienen muchos productos listados para usar DA14580»,* dijeron los investigadores.
>
> *«Por lo tanto, todos estos productos son potencialmente vulnerables al ataque L2CAP truncado. Aún peor, Syqe Medical Ltd. y su plataforma de inhalación de administración de medicamentos programable (Syque Inhaler v01), se ve afectada junto con los últimos productos relacionados con marcapasos de Medtronic Inc».*

Según el informe, los investigadores revelaron las vulnerabilidades el año pasado a todos los proveedores afectados, muchos de los cuales ya lanzaron parches para sus respectivos SoC.