Se reveló un conjunto de nuevas vulnerabilidades de seguridad en pilas de Bluetooth comerciales que podrían permitir a un adversario ejecutar código arbitrario y, lo que resulta peor, bloquear los dispositivos mediante ataques de denegación de servicio (DoS).

Denominadas de forma colectiva como BrakTooth (en referencia a la palabra noruega Brak, que se traduce como accidente), las 16 vulnerabilidades de seguridad abarcan 13 conjuntos de chips Bluetooth de 11 proveedores como Intel, Qualcomm, Zhuhai Jieli Technology y Texas Instruments, que cubren alrededor de 1400 o más productos comerciales, incluidas computadoras portátiles, teléfonos inteligentes, controladores lógicos programables y dispositivos de IoT.

Las vulnerabilidades fueron reveladas por investigadores del Grupo de Investigación ASSET (Automated Systems Security) de la Universidad de Tecnología y Diseño de Singapur (SUTD).

> *«Todas las vulnerabilidades pueden activarse sin ningún emparejamiento o autenticación previa. El impacto de nuestras vulnerabilidades descubiertas se clasifica en (I) fallas y (II) interbloqueos. Las fallas generalmente desencadenan una afirmación fatal, fallas de segmentación debido a un búfer o desbordamiento de pila dentro del firmware de SoC. Los interbloqueos, en contraste, conducen al dispositivo de destino a una condición en la que no sea posible ninguna otra comunicación BT»,* dijeron los investigadores.

La más grave de las 16 vulnerabilidades es CVE-2021-28139, que afecta al SoC ESP32 que se utiliza en muchos dispositivos basados en Bluetooth que van desde la electrónica de consumo hasta los equipos industriales. Debido a la falta de una verificación fuera de los límites en la biblioteca, la falla permite a un atacante inyectar código arbitrario en dispositivos vulnerables, incluido el borrado de sus datos NVRAM.

Otras vulnerabilidades podrían provocar que la funcionalidad de Bluetooth se deshabilite por

completo mediante la ejecución de código arbitrario, o causar una condición de denegación de servicio en computadoras portátiles y teléfonos inteligentes que emplean Intel AX200 SoC.

> *«Esta vulnerabilidad permite a un atacante desconectar por la fuerza los dispositivos BT esclavos actualmente conectados a AX200 en computadoras portátiles Windows o Linux. De forma similar, los teléfonos Android como Pocophone F1 y Oppo Reno 5G experimentan interrupciones de BT»,* agregaron los investigadores.

Además, se podría abusar de una tercera colección de fallas descubiertas en los parlantes, auriculares y módulos de audio Bluetooth para congelar e incluso apagar por completo los dispositivos, lo que requiere que los usuarios los vuelvan a encender de forma manual. Es preocupante que todos los ataques de BrakTooth antes mencionados podrían llevarse a cabo con un rastreador de paquetes Bluetooth fácilmente disponible que cuesta menos de 15 dólares.

Aunque Espressif, Infineon (Cypress) y Bluetrum Technology lanzaron parches de firmware para rectificar las vulnerabilidades identificadas, se dice que Intel, Qualcomm y Zhuhai Jieli Technology están investigando las vulnerabilidades o en el proceso de preparación de actualizaciones de seguridad. Texas Instruments por otro lado, no tiene la intención de lanzar una solución a menos que *«lo exijan los clientes».*

El grupo ASSET también ha puesto a disposición una herramienta de prueba de concepto (PoC), que pueden utilizar los proveedores que producen SoC, módulos y productos Bluetooth para replicar las vulnerabilidades y validar contra los ataques de BrakTooth.