Más de mil millones de dispositivos Bluetooth, incluyendo teléfonos inteligentes, laptops, dispositivos IoT inteligentes y dispositivos industriales, se han encontrado vulnerables a un fallo grave que podría permitir a los hackers espiar los datos transmitidos entre los dispositivos.

La vulnerabilidad CVE-2019-9506, reside en la forma en que el *«protocolo de negociación de clave de cifrado»* permite que dos dispositivos Bluetooth BR/EDR elijan un valor de entropía para las claves de cifrado mientras se emparejan para asegurar su conexión.

Conocida como Ataque de Negociación Clave de Bluetooth (KNOB), la vulnerabilidad podría permitir que los atacantes remotos cercanos a dispositivos específicos intercepten, supervisen o manipulen el tráfico cifrado de Bluetooth entre dos dispositivos emparejados.

El Bluetooth BR/EDR (velocidad básica/velocidad de datos mejorada, también conocido como Bluetooth Classic), es un estándar de tecnología inalámbrica que generalmente se ha diseñado para una conexión inalámbrica continua de corto alcance, como la transmisión de audio a auriculares o altavoces portátiles.

Desde el punto de vista de la seguridad, la especificación central del protocolo Bluetooth BR/EDR admite claves de cifrado con entropía entre 1 y 16 bytes/octetos, donde el valor más alto significa más seguridad.

Sin embargo, los investigadores encuentran que la negociación de entropía, que dispositivos realizan a través del Protocolo de Administrador de Enlace (LMP), no está encriptada ni autenticada, y puede ser secuestrada o manipulada por aire.

Funcionamiento de la vulnerabilidad de negociación de claves BR/EDR

La vulnerabilidad Bluetooth descubierta podría permitir a un atacante remoto engañar a dos dispositivos específicos para que acuerden una clave de cifrado con solo 1 byte (8 bits) de entropía, lo que eventualmente facilitaría la fuerza bruta de las claves de cifrado negociadas.

> *«Por ejemplo, suponga que hay dos controladores que intentan establecer una conexión: Alice y Bob. Después de autenticar la clave de enlace, Alice propone que ella y Bob usen 16 bytes de entropía. Este número N, podría estar entre 1 y 16 bytes. Bob puede aceptar esto, rechazar esto y abortar la negociación, o proponer un valor menor»,* dice un aviso publicado por el Centro de Coordinación del CERT.
>
> *«Bob podría proponer un valor N menor porque el controlador no admite la mayor cantidad de bytes propuesta por Alice. Después de proponer una cantidad menor, Alice puede aceptarlo y solicitar activar el cifrado de capa de enlace con Bob, que Bob puede aceptar».*

Sin embargo, al explotar la vulnerabilidad reportada *«un atacante, Charlie, podría obligar a Alice y Bob a usar una N más pequeña interceptando la solicitud de propuesta de Alice a Bob y cambiando N».*

Una vez descifrado, el atacante puede capturar pasivamente mensajes cifrados que se transmiten a través del tráfico de Bluetooth, descifrar el texto cifrado e inyectar texto cifrado válido, todo en tiempo real.

Además, también es importante tener en cuenta que para que un ataque se considere exitoso, se debe considerar:

- Ambos dispositivos Bluetooth deben establecer una conexión BR/EDR
- Ambos dispositivos Bluetooth deben ser vulnerables al defecto, el atacante debería poder bloquear las transacciones directas entre los dispositivos mientras se empareja, y el ataque debe realizarse durante la negociación o renegociación de una conexión de dispositivo emparejado.

Además, el aviso oficial publicado por Bluetooth.com también dice:

> *«Dado que no todas las especificaciones de Bluetooth exigen una longitud mínima de clave de cifrado, es posible que algunos proveedores hayan desarrollado productos Bluetooth donde la longitud de la clave de cifrado utilizada en un BR/EDR, la conexión podría establecerse mediante un dispositivo de ataque a un solo octeto».*

Proveedores afectados / software / SO y actualizaciones

Esta vulnerabilidad fue descubierta por un equipo de investigadores, entre ellos, Daniele Antonioli de SUTD, el Dr. Nils Ole Tippenhauer de CISPA y el profesor Kasper Rasmussen de la Universidad de Oxford.

> *«Evaluamos el ataque KNOB en más de 14 chips Bluetooth de diferentes proveedores como Intel, Broadcom, Apple y Qualcomm. Todos los chips aceptan 1 byte de entropía, excepto el chip Apple W1 que acepta 7 bytes de entropía»*, dijeron los investigadores en un documento detallado.

Para mitigar el ataque KNOB, los encargados del mantenimiento de las especificaciones de Bluetooth han recomendado encarecidamente a los fabricantes de dispositivos y vendedores de software que apliquen una longitud mínima de clave de cifrado de 7 octetos para las conexiones BR/EDR.

Para reportar dicha vulnerabilidad, varios proveedores afectados ya comenzaron a lanzar actualizaciones de seguridad para sus sistemas operativos, firmware y software, que incluyen:

- Microsoft para Windows
- Cisco para teléfonos IP y Webex
- Google para Android
- Apple para MacOS, iOS y WatchOS

- BlackBerry