Académicos de la École Polytechnique Fédérale de Lausanne (EPFL), revelaron una vulnerabilidad de seguridad en Bluetooth que permitiría a un hacker falsificar un dispositivo emparejado de forma remota, exponiendo más de mil millones de dispositivos modernos a piratas informáticos.

Dichos ataques, denominados como ataques de suplantación de identidad Bluetooth o BIAS, se refieren a Bluetooth Classic, que admite velocidad básica (BR) y velocidad de datos mejorada (EDR) para la transferencia inalámbrica de datos entre dispositivos.

> *«La especificación Bluetooth contiene vulnerabilidades que permiten llevar a cabo ataques de suplantación durante el establecimiento de conexión segura. Tales vulnerabilidades incluyen la falta de autenticación mutua obligatoria, el cambio de roles excesivamente permisivo y una rebaja del procedimiento de autenticación»*, dijeron los investigadores.

Debido al impacto generalizado de la vulnerabilidad, los investigadores afirmaron que divulgaron de forma responsable los hallazgos al Grupo de Interés Especial Bluetooth (SIG), la organización que supervisa el desarrollo de los estándares de Bluetooth en diciembre de 2019.

Ataque BIAS

Para que BIAS tenga éxito, un dispositivo atacantes debería estar dentro del alcance inalámbrico de un dispositivo Bluetooth vulnerable que haya establecido previamente una conexión BR/EDR con otro dispositivo Bluetooth cuya dirección sea conocida por el atacante.

La falla proviene de cómo dos dispositivos previamente emparejados manejan la clave a largo plazo, también conocida como clave de enlace, que se utiliza para autenticar mutuamente los dispositivos y activar una conexión segura entre ellos.

La clave de enlace también garantiza que los usuarios no tengan que emparejar sus dispositivos cada vez que se produce una transferencia de datos entre, por ejemplo, un auricular inalámbrico y un teléfono, o entre dos computadoras portátiles.

El atacante, entonces, puede explotar el error para solicitar una conexión a un dispositivo vulnerable falsificando la dirección Bluetooth del otro extremo, y viceversa, falsificando así la identidad y obtieniendo acceso completo a otro dispositivo sin contar con la clave de emparejamiento a largo plazo que se utiliza para establecer la conexión.

Además, el sesgo puede combinarse con otros ataques, incluyendo el mando (Tecla de Negociación de Bluetooth), que se produce cuando una parte tercera fuerza a dos o más víctimas a un acuerdo acerca de una clave de cifrado con la entropía reducida, lo que permite al atacante forzar la clave de cifrado mediante fuerza bruta, y utilizarla para descifrar las comunicaciones.

Dispositivos afectados

Con la mayoría de los dispositivos Bluetooth compatibles con el estándar afectados por la vulnerabilidad, los investigadores afirmaron que probaron el ataque contra hasta 30 dispositivos, incluidos teléfonos inteligentes, tabletas, computadoras portátiles, auriculares y computadoras de una sola placa como Raspberry Pi. Se encontró que todos los dispositivos eran vulnerables a ataques BIAS.

Bluetooth SIG dijo que está actualizando la Especificación Core de Bluetooth para *«evitar una degradación de las conexiones seguras al cifrado heredado»*, lo que permite al atacante iniciar *«un cambio de rol maestro-esclavo para colocarse en el rol maestro y convertirse en el iniciador de autenticación».*

> *«Los ataques de BIAS son los primeros problemas de descubrimiento relacionados con los procedimientos de autenticación de establecimiento de conexión segura de Bluetooth, interruptores de roles adversos y degradaciones de conexiones seguras.*

> *Los ataques BIAS son sigilosos, ya que el establecimiento de una conexión segura Bluetooth no requiere la interacción del usuario»,* dijeron los investigadores.