Nuevas investigaciones han revelado una serie de ataques innovadores que comprometen la seguridad avanzada y futura de Bluetooth Classic, dando lugar a escenarios de adversarios en medio (AitM) entre dos pares que ya están conectados.

Estos problemas, agrupados bajo el nombre de BLUFFS, afectan a la Especificación Central de Bluetooth desde la versión 4.2 hasta la 5.4. Están identificados con el CVE-2023-24023 (puntuación CVSS: 6.8) y se dieron a conocer de manera responsable en octubre de 2022.

Daniele Antonioli, investigador de EURECOM, explicó en un estudio publicado el mes pasado que estos ataques *«facilitan la suplantación de dispositivos y la intervención en el medio a lo largo de sesiones al comprometer solo una clave de sesión».*

Esta amenaza es posible gracias a la explotación de dos nuevas vulnerabilidades en el mecanismo de derivación de claves de sesión del estándar Bluetooth, lo que permite la derivación de la misma clave a lo largo de distintas sesiones.

Mientras que la seguridad avanzada en protocolos criptográficos de acuerdo de claves garantiza que las comunicaciones pasadas no sean reveladas incluso si las claves privadas de un intercambio particular son descubiertas por un atacante pasivo, la seguridad futura (también conocida como seguridad hacia atrás) asegura la confidencialidad de los mensajes futuros en caso de que las claves anteriores se vean comprometidas.

En términos sencillos, la seguridad avanzada protege las sesiones pasadas contra posibles compromisos futuros de claves.

El ataque se lleva a cabo aprovechando cuatro vulnerabilidades arquitectónicas, que incluyen las dos ya mencionadas, presentes en la especificación del proceso de establecimiento de sesión de Bluetooth. Esto permite derivar una clave de sesión débil, la cual puede ser posteriormente forzada mediante ataques de fuerza bruta para falsificar a víctimas arbitrarias.

Un atacante AitM que se haga pasar por el dispositivo emparejado podría entonces negociar

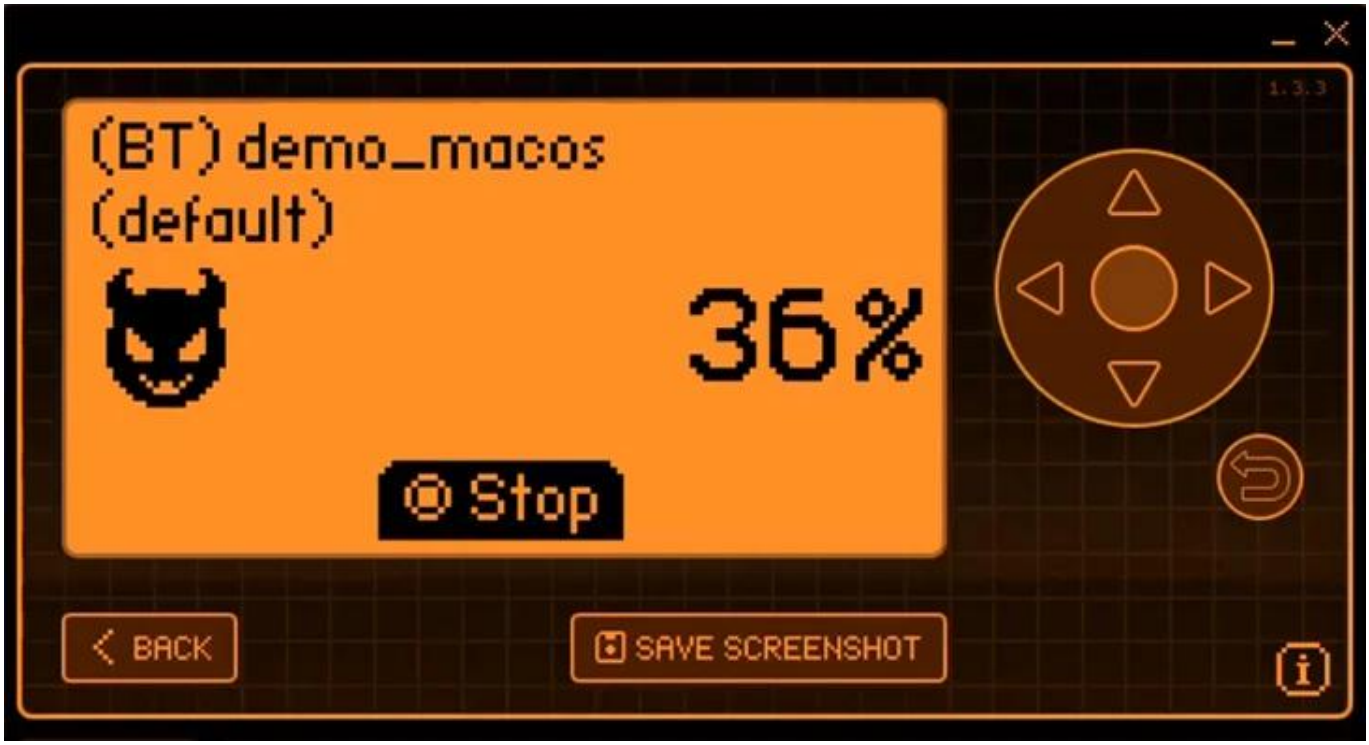
una conexión con el otro extremo para establecer un procedimiento de cifrado posterior utilizando un cifrado heredado.

Al hacerlo, *«un atacante en proximidad podría asegurarse de que se utilice la misma clave de cifrado para cada sesión mientras está en proximidad y forzar la longitud de la clave de cifrado más baja admitida»,* mencionó el Grupo de Interés Especial de Bluetooth (SIG).

> *«Cualquier implementación BR/EDR que cumpla con los estándares se espera que sea vulnerable a este ataque en el establecimiento de claves de sesión. Sin embargo, el impacto podría limitarse al denegar el acceso a los recursos del host desde una sesión degradada o al garantizar suficiente entropía clave para hacer que la reutilización de claves de sesión sea de utilidad limitada para un atacante».*

Además, un atacante puede aprovechar estas debilidades para forzar la clave de cifrado en tiempo real, posibilitando así ataques de inyección en vivo en el tráfico entre pares vulnerables.

El éxito del ataque, no obstante, presupone que un dispositivo atacante se encuentra dentro del rango inalámbrico de dos dispositivos Bluetooth vulnerables que inician un procedimiento de emparejamiento, y que el adversario puede capturar paquetes Bluetooth tanto en texto plano como cifrados, conociendo la dirección Bluetooth de la víctima y creando paquetes Bluetooth.



Como medidas de mitigación, SIG recomienda que las implementaciones de Bluetooth rechacen conexiones a nivel de servicio en un enlace de banda base cifrado con longitudes de clave por debajo de 7 octetos. Asimismo, sugiere que los dispositivos operen en *«Modo Solo Conexiones Seguras»* para garantizar una fuerza clave suficiente, y que el emparejamiento se realice a través del modo *«Conexiones Seguras»* en lugar del modo heredado.

Este hallazgo se produce en medio de la revelación de ThreatLocker sobre un ataque de suplantación de Bluetooth que puede explotar el mecanismo de emparejamiento para obtener acceso inalámbrico a sistemas Apple macOS a través de la conexión Bluetooth y lanzar una shell inversa.