Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°285	Fecha: 29-11-72023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El nuevo ataque BLUFFS permite a los atacantes secuestrar conexiones Bluetooth		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El Bluetooth es una tecnología que utilizamos constantemente en nuestro día a día. Puede que lo uses en auriculares, altavoces, mandos, sensores que tienes en casa. Está presente en muchos dispositivos y, por eso, cuando surge una vulnerabilidad puede ser un problema importante.

Hablamos de miles de millones de dispositivos en todo el mundo que pueden ser vulnerables a estos ataques. Aquí podemos incluir aparatos tan diversos como ordenadores, móviles, relojes inteligentes, etc. Son muchos los dispositivos que usamos en nuestro día a día y que utilizan esta tecnología en las comunicaciones.

A continuación, se indica cómo están utilizando un nuevo ataque para secuestrar conexiones Bluetooth.

2. DETALLES:

Se trata de ataques conocidos como BLUFFS. Pueden romper la privacidad entre conexiones Bluetooth y llegar a suplantar la identidad de los dispositivos, además de realizar ataque Man in The Middle. Se aprovechan de dos vulnerabilidades existentes en el estándar Bluetooth, que están relacionadas con cómo se derivan las claves de sesión para descifrar los datos.

Estas fallas, según indica Daniele Antonioli, investigador detrás del descubrimiento, no son específicas de las configuraciones de hardware o software, sino que son arquitectónicas, lo que significa que afectan a Bluetooth en un nivel fundamental. Han sido registrados como CVE-2023-24023 y afectan a las versiones que van del Bluetooth 4.2 al Bluetooth 5.4. Por tanto, son muchos los dispositivos que pueden estar afectados.

BLUFFS es una serie de exploits dirigidos a Bluetooth, cuyo objetivo es comprometer la privacidad de las comunicaciones tanto pasadas como futuras entre los dispositivos.

Esto se logra explotando cuatro fallas en el proceso de derivación de claves de sesión, dos de las cuales son nuevas, para forzar la derivación de una clave de sesión (SKC) corta, por lo tanto, débil y predecible.

Utiliza la fuerza bruta para romper la clave y descifrar así las comunicaciones.

Para que esto sea posible, el atacante debe estar en el rango de alcance de los dispositivos Bluetooth y se hace pasar por uno de ellos para negociar la clave de sesión débil.

En total, son 6 los ataques BLUFFS que fueron desarrollados por los investigadores de Eurecom, las cuales cubren varias combinaciones de ataques de suplantación de identidad y MitM, que funcionan independientemente de si las víctimas admiten Secure Connections (SC) o Legacy Secure Connections (LSC).

- A1: Falsificación de una central LSC
- A2: falsificación de un periférico LSC
- A3: Víctimas de MitM LSC
- A4: Falsificar una SC Central
- A5: Falsificación de un periférico SC
- A6: Víctima de MitM SC

Los investigadores desarrollaron y compartieron un conjunto de herramientas en GitHub que demuestra la eficacia de BLUFFS. Incluye un script Python para probar los ataques, los parches ARM, el analizador y las muestras PCAP capturadas durante sus pruebas.

El documento de Eurecom presenta los resultados de las pruebas de BLUFFS en varios dispositivos, incluidos teléfonos inteligentes, auriculares y computadoras portátiles, que ejecutan las versiones de Bluetooth 4.1 a 5.2. Se confirmó que todos ellos eran susceptibles a al menos tres de seis ataques de BLUFFS.

Chip	Device(s)	BTv	A1	A2	A3	A4	A5	A6
LSC Victims								
Bestechnic BES2300	Pixel Buds A-Series[3]	5.2	✓	✓	✓	✓	✓	✓
Apple H1	AirPods Pro	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW20721	Jaybird Vista	5.0	✓	✓	✓	✓	✓	✓
CSR/Qualcomm BC57H687C-GITM-E4	Bose SoundLink[1,2]	4.2	✓	✓	✓	✓	✓	✓
Intel Wireless 7265 (rev 59)	Thinkpad X1 3rd gen	4.2	✓	✓	✓	✓	✓	✓
CSR n/a	Logitech BOOM 3[1]	4.2	✓	×	✓	✓	×	✓
SC Victims								
Infineon CYW20819	CYW920819EVB-02	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW40707	Logitech MEGABLAST	4.2	✓	✓	✓	✓	✓	✓
Qualcomm Snapdragon 865	Mi 10T[4]	5.2	✓	✓	✓	×	×	×
Apple/USI 339S00761	iPhones 12[4], 13[4]	5.2	✓	✓	✓	×	×	×
Intel AX201	Portege X30-C[4]	5.2	✓	✓	✓	×	×	×
Broadcom BCM4389	Pixel 6[4]	5.2	✓	✓	✓	×	×	×
Intel 9460/9560	Latitude 5400[4]	5.0	✓	✓	✓	×	×	×
Qualcomm Snapdragon 835	Pixel 2[4]	5.0	✓	✓	✓	×	×	×
Murata 339S00199	iPhone 7[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 821	Pixel XL[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 410	Galaxy J5[4]	4.1	✓	✓	✓	×	×	×

3. RECOMENDACIONES:

- Mantener actualizados todos los sistemas en los dispositivos que usen tecnología Bluetooth.
- Rechazar las conexiones de nivel de servicio en un enlace de banda base cifrado con fortalezas de clave inferiores a 7 octetos. Para implementaciones capaces de utilizar siempre el Modo de seguridad 4 Nivel 4, las implementaciones deben rechazar conexiones de nivel de servicio en un enlace de banda base cifrado con una intensidad de clave inferior a 16 octetos.
- Configurar para que los dispositivos siempre funcionen en modo Sólo conexiones seguras.

Fuente de Información:	• hxxps://www.redeszone.net/noticias/seguridad/ataque-bluetooth-bluffs-dispositivos/ • hxxps://www.bleepingcomputer.com/news/security/new-bluffs-attack-lets-attackers-hijack-bluetooth-connections/#google_vignette • hxxps://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/bluffs-vulnerability/