Investigadores de seguridad cibernética demostraron una nueva técnica de ataque que permite aprovechar el componente Bluetooth de un dispositivo para extraer directamente las contraseñas de red y manipular el tráfico en un chip WiFi.

Los nuevos ataques funcionan contra los llamados *«chips combinados»,* que son chips especializados que están equipados para manejar distintos tipos de comunicaciones inalámbricas basadas en ondas de radio, como WiFi, Bluetooth y LTE.

«Proporcionamos evidencia empírica de que la coexistencia, es decir, la coordinación de transmisiones inalámbricas de tecnología cruzada, es una superficie de ataque inexplorada», dijo un grupo de investigadores del Laboratorio de Redes Móviles Seguras de la Universidad Técnica de Darmstadt y la Universidad de Brescia.

> *«En lugar de escalar directamente al sistema operativo móvil, los chips inalámbricos pueden escalar sus privilegios a otros chips inalámbricos explotando los mismos mecanismos que utilizan para arbitrar su acceso a los recursos que comparten, es decir, la antena transmisora y el medio inalámbrico».*

La coexistencia se refiere a un mecanismo en el que Bluetooth, WiFi y LTE comparten los mismos componentes y recursos, por ejemplo, antena o espectro inalámbrico, lo que requiere que dicho estándares de comunicación coordinen el acceso al espectro para evitar colisiones cuando operan en la misma frecuencia. Los proveedores de chipsets utilizan este principio para permitir que WiFi y Bluetooth funcionen virtualmente al mismo tiempo.

Aunque estos chips inalámbricos combinados son clave para compartir espectro de alto rendimiento, las interfaces de coexistencia también representan un riesgo de canal lateral, como lo demostró el mismo grupo de investigadores en la conferencia de seguridad de Black Hat el año pasado, permitiendo de forma efectiva que una parte malintencionada recopile detalles de otras tecnologías inalámbricas compatibles con el chip combinado.

Apodado como «Spectra», la clase de vulnerabilidad se basa en el hecho de que las

transmisiones ocurren al mismo espectro y los chips inalámbricos necesitan arbitrar el acceso al canal. Esto rompe la separación entre WiFi y Bluetooth para dar como resultado la denegación de servicio en el acceso al espectro, la divulgación de información e incluso permitir escaladas laterales de privilegios desde un chip Bluetooth a la ejecución de código en un chip WiFi.

> *«El chip de WiFi cifra el tráfico de la red y mantiene las credenciales de WiFi actuales, proporcionando así al atacante más información. Además, un atacante puede ejecutar código en un chip WiFi aún si no está conectado a una red inalámbrica»,* dijeron los investigadores.

Además, los investigadores descubrieron que es posible que un adversario con control sobre el núcleo de WiFi observe los paquetes Bluetooth, lo que a su vez, permite determinar los tiempos de pulsación de teclas en los teclados Bluetooth, lo que finalmente otorga al atacante la capacidad de reconstruir el texto ingresado usando el teclado.

Aunque algunos de los escenarios de ataque se informaron por primera vez a los proveedores en agosto de 2019, las fallas de coexistencia siguen sin ser respaldadas en los SoC de Broadcom hasta ahora.

> *«En noviembre de 2021, más de dos años después de reportar el primer error de coexistencia, los ataques de coexistencia, incluyendo la ejecución de código, todavía funcionan en chips Broadcom actualizados. Esto pone en relieve lo difícil que es solucionar estos problemas en la práctica»*, dijeron los académicos.

Para minimizar el riesgo de dichos ataques inalámbricos, se recomienda que los usuarios eliminen los emparejamientos de Bluetooth innecesarios, eliminen las redes WiFi no utilizadas y se restrinja el uso de celulares con WiFi en espacios públicos.

> *«Los planes de datos celulares se volvieron más asequibles durante los últimos años y la cobertura de la red celular aumentó. Deshabilitar el WiFi de forma predeterminada y habilitarlo solo cuando se usan redes confiables puede considerarse una buena práctica de seguridad, incluso si es engorroso*», dijeron los investigadores.