Se han descubierto importantes vulnerabilidades en el módulo WiFi Realtek RTL8195A que podrían haber sido explotadas para obtener acceso de root y tomar el control completo de las comunicaciones inalámbricas de un dispositivo.

Las seis vulnerabilidades fueron informadas por investigadores de la compañía de seguridad de IoT israelí Vdoo.

El Realtek RTL8195A es un módulo de hardware de WiFi autónomo de bajo consumo de energía dirigido a dispositivos integrados utilizados en distintas industrias, como la agricultura, el hogar inteligente, atención médica, juegos y sectores automotrices.

También utiliza una API *«Ameba»*, que permite a los desarrolladores comunicarse con el dispositivo a través de WiFi, HTTP y MQTT, un protocolo de mensajería liviano para pequeños sensores y dispositivos móviles.

Aunque los problemas descubiertos por Vdoo se verificaron solo en RTL8195A, los investigadores dijeron que también se extienden a otros módulos, incluidos RTL8711AM, RTL8711AF y RTL8710AF.

Las fallas se refieren a una combinación de desbordamiento de pila y lecturas fuera de límites que se derivan del mecanismo de enlace de cuatro vías WPA2 del módulo WiFi durante la autenticación.

La más crítica, es una vulnerabilidad de desbordamiento de búfer (CVE-2020-9395) que permite a un atacante en la proximidad de un módulo RTL8195 hacerse cargo por completo del módulo, sin tener que conocer la contraseña de la red WiFi y todo independiente de si el módulo actúa como punto de acceso WiFi o cliente.

Se puede abusar de otras dos vulnerabilidades para organizar una denegación de servicio, mientras que otro conjunto de vulnerabilidades, incluyendo CVE-2020-25854, podría permitir la explotación de dispositivos cliente WiFi y ejecutar código arbitrario.

Por lo tanto, en uno de los posibles escenarios de ataque, un adversario cono conocimiento previo de la frase de contraseña para la red WiFi WPA2 a la que está conectado el dispositivo víctima, puede crear un AP malicioso al rastrear el SSID de la red y la clave de tránsito por parte (PTK), que se utiliza para cifrar el tráfico entre un cliente y el AP y forzar al objetivo a conectarse al nuevo AP y ejecutar código malicioso.

Realtek respondió con Ameba Arduino 2.0.8 con parches para las seis vulnerabilidades encontradas por Vdoo. Cabe mencionar que las versiones de firmware lanzadas después del 21 de abril de 2020 ya cuentan con las protecciones necesarias para frustrar los ataques de adquisición.

> *«Un problema fue descubierto en dispositivos Realtek RTL8195AM, RTL8711AM, RTL8711AF y RTL8710AF antes de 2.0.6. Existe un desbordamiento de búfer basado en pila en el código del cliente que se encarga del protocolo de enlace de 4 vías de WPA2 a través de un paquete EAPOL-Key mal formado con un búfer de datos clave largo»*, dijo la compañía.