Se han revelado tres fallas de diseño y de implementación múltiple en el estándar técnico IEEE 802.11 que sustenta WiFi, permitiendo potencialmente que un adversario tome el control de un sistema y robe datos confidenciales.

Denominadas como FragAttacks (FRagmentation y AGregation), las vulnerabilidades afectan a todos los protocolos de seguridad WiFi, desde Wired Equivalent Privacy (WEP) hasta WiFi Protectes Access 3 (WPA3), por lo que prácticamente todos los dispositivos inalámbricos habilitados están en riesgo de ataque.

> *«Un adversario que se encuentra dentro del alcance de radio de una víctima puede abusar de estas vulnerabilidades para robar información del usuario o atacar dispositivos. Los experimentos indican que todos los productos WiFi se ven afectados por al menos una vulnerabilidad y que la mayoría de los productos se ven afectados por varias vulnerabilidades»,* dijo Mathy Vanhoef, académico de seguridad de la Universidad de Nueva York en Abu Dhabi.

IEEE 802.11 proporciona la base para todos los dispositivos modernos que utilizan la familia de protocolos de red WiFi, lo que permite que las computadoras portátiles, tabletas, impresoras, teléfonos inteligentes, altavoces inteligentes y otros dispositivos se comuniquen entre sí y accedan a Internet a través de un enrutador inalámbrico.

Introducido en enero de 2018, WPA3 es un protocolo de seguridad de tercera generación que se encuentra en la mayoría de los dispositivos WiFi con varias mejoras, como una autenticación sólida y una mayor capacidad criptográfica para proteger las redes informáticas inalámbricas.

Según Vanhoef, los problemas se derivan de errores de programación *«generalizados»* codificados en la implementación del estándar, con algunos defecto que se remontan a 1997. Las vulnerabilidades tienen que ver con la forma en que el estándar fragmenta y agrega marcos, lo que permite a los atacantes inyectar paquetes arbitrarios y engañar a una víctima para que utilice un servidor DNS malicioso, o falsificar los marcos para desviar datos.

La lista de vulnerabilidades es la siguiente:

- CVE-2020-24588: Aceptación de tramas A-MSDU que no son SPP
- CVE-2020-24587: Reensamblaje de fragmentos cifrados con diferentes claves
- CVE-2020-24856: No se borran fragmentos de la memoria cuando se reconecta a una red
- CVE-2020-26145: Aceptación de fragmentos de transmisión de texto sin formato como fotogramas completos (en una red cifrada)
- CVE-2020-26144: Aceptación de tramas A-MSDU de texto sin formato que comienzan con un encabezado RFC1042 con EtherType EAPOL (en una red cifrada)
- CVE-2020-26140: Aceptación de marcos de datos de texto sin formato en una red protegida
- CVE-2020-16143: Aceptación de marcos de datos de texto plano fragmentados en una red protegida
- CVE-2020-26139: Reenvío de tramas EAPOL aunque el remitente aún no esté autenticado
- CVE-2020-26146: Reensamblaje de fragmentos cifrados con números de paquete no consecutivos
- CVE-2020-26147: Reensamblaje de fragmentos mixtos cifrados y/o de texto sin formato
- CVE-2020-26142: Procesamiento de fotogramas fragmentados como fotogramas completos
- CVE-2020-26141: No verificar el TKIP MIC de tramas fragmentadas

Un pirata informático puede aprovechar estas vulnerabilidades para inyectar paquetes de red arbitrarios, interceptar y exfiltrar datos de usuario, lanzar ataques de denegación de servicio e incluso posiblemente descifrar paquetes en redes WPA o WPA2.

> *«Si se pueden inyectar paquetes de red hacia un cliente, se puede abusar de esto para engañar al cliente para que use un servidor DNS malicioso. Si los paquetes de red se pueden inyectar hacia un punto de acceso, el adversario puede abusar de*

> *esto para evitar el NAT/Firewall y conectarse directamente a cualquier dispositivo en la red local»*, explicó Vanhoef.

En un escenario de ataque hipotético, estas vulnerabilidades pueden explotarse como un trampolín para lanzar ataques avanzados, permitiendo que un atacante se apodere de una máquina obsoleta con Windows 7 dentro de una red local. Pero en una nota más brillante, las fallas de diseño son difíciles de explotar, debido a que requieren la interacción del usuario o solo son posibles cuando se utilizan configuraciones de red poco comunes.

Los hallazgos se han compartido con WiFi Alliance, después de lo cual se prepararon actualizaciones de firmware durante un período de divulgación coordinado de 9 meses. Microsoft por su parte, lanzó correcciones para algunas de las fallas (CVE-2020-24857, CVE-2020-24588 y CVE-2020-26144) como parte de su actualización Patch Tuesday para mayo de 2021. Vanhoef dijo que un kernel de Linux actualizado está en proceso para distribuciones con soporte activo.

Esta no es la primera vez que Vanhoef ha demostrado vulnerabilidades graves en el estándar WiFi. En 2017, el investigador reveló lo que se llama KRACKs (Key Reinstallation AttACKs) en el protocolo WPA2, lo que permite a un atacante leer información confidencial y robar números de tarjetas de crédito, contraseñas, mensajes y otros datos.

> *«Curiosamente, nuestro ataque de agregación podría haberse evitado si los dispositivos hubieran implementado mejoras de seguridad opcionales antes. Esto destaca la importancia de implementar mejoras de seguridad antes de que se conozcan los ataques prácticos. Las dos fallas de diseño basadas en la fragmentación fueron, en un alto nivel, causadas por no separar de forma adecuada los distintos contextos de seguridad. De esto se aprende que separar adecuadamente los contextos de seguridad es un principio importante a tener en cuenta a la hora de diseñar protocolos»,* agregó Vanhoef.

Se puede tener acceso a las mitigaciones para FragAttacks de otras compañías como Cisco, HPE/Aruba Networks, Juniper Networks y Sierra Wireless en el aviso publicado por el Industry Consortium for Advancement of Security on the Internet (ICASI).

> *«No existe evidencia que muestre que las vulnerabilidades se utilizan contra los usuarios de WiFi maliciosamente, y estos temas se mitigan a través de las actualizaciones del dispositivo rutinarias que permiten la detección de las transmisiones sospechosas o mejoran la adherencia a las prácticas de implementación de seguridad recomendadas»*, dijo WiFi Alliance.