Ha pasado casi un año desde el lanzamiento del nuevo estándar de seguridad WiFi WPA3 y los investigadores ya descubrieron varias vulnerabilidades graves en el protocolo de seguridad inalámbrica que podrían permitir a los hackers recuperar la contraseña de la red.

WPA, o Acceso Protegido a WiFi, es un estándar diseñado para autenticar dispositivos inalámbricos utilizando el protocolo de Estándar de Cifrado Avanzado (AES) y está pensado para evitar que los piratas informáticos tengan acceso a sus datos inalámbricos.

El protocolo WiFi Protected Access III (WPA3) se lanzó en un intento de solucionar las fallas técnicas del protoclo WPA2 desde abajo, que durante mucho tiempo se consideró como inseguro y vulnerable a KRACK (ataque de reinstalación de clave).

Aunque WPA3 se basa en un apretón de manos más seguro, conocido como DragonFly, que apunta a proteger las redes WiFi contra ataques de diccionario fuera de línea, los investigadores de seguridad Mathy Vanhoef y Eyal Ronen encontraron debilidades en la implementación temprana de WPA3-Personal, lo que permitió a un atacante recuperar contraseñas de WiFi abusando de la sincronización o las fugas de canal lateral.

> *«Concretamente, los atacantes pueden leer la información que se suponía que WPA3 cifraba de forma segura. Se puede abusar de ella para robar información sensible transmitida, como números de tarjetas de crédito, contraseñas, mensajes de chat, correos electrónicos, etc»*, dijeron los investigadores.

En un artículo de investigación, apodado DragonBlood, publicado hoy, los investigadores detallaron dos tipos de fallas de diseño en WPA3: la primera lleva a ataques de downgrade y la segunda a fugas de canal lateral.

Dado que el protocolo WPA2 con 15 años de antigüedad ha sido ampliamente utilizado por miles de millones de dispositivos, la adopción generalizada de WPA3 no se realizará de la noche a la mañana. Para admitir dispositivos antiguos, los dispositivos con certificación WPA3 ofrecen un *«modo de operación de transición»* que se puede configurar para aceptar

conexiones con WPA3-SAE y WPA2.

Los investigadores descubren que el modo de transición es vulnerable a los ataques de degradación, que los atacantes pueden abusar para configurar un AP no autorizado que solo admite WPA2, lo que obliga a los dispositivos compatibles con WPA3 a conectarse mediante el protocolo de enlace de 4 vías del inseguro WPA2.

> *«También descubrimos un ataque de baja calificación contra SAE (Autenticación Simultánea de la Igualdad de Manos, comúnmente conocida como Libélula), donde podemos forzar a un dispositivo a utilizar una curva elíptica más débil de la que normalmente se usaría»*, dijeron los investigadores.

Además, no se necesita una posición de hombre en el medio para llevar a cabo un ataque de baja calificación. En su lugar, los atacantes solo necesitan conocer el SSID de la red WPA3-SAE.

Los investigadores también detallan dos ataques de canal lateral (ataques basados en caché CVE-2019-9494 y basados en sincronización CVE-2019-9494, contra el método de codificación de contraseña de Dragonfly que podría permitir a los atacantes realizar un ataque de partición de contraseña, similar a un ataque de diccionario fuera de línea, para obtener la contraseña del WiFi.

> *«Para nuestro ataque de partición de contraseñas, debemos registrar varios acuerdos con diferentes direcciones MAC. Podemos obtener acuerdos con diferentes direcciones MAC dirigiéndonos a múltiples clientes en la misma red. Solo podemos atacar a un cliente, podemos configurar puntos de acceso no autorizados con el mismo SSID pero con una dirección MAC falsificada»*, agregaron.

Además de esto, los investigadores también documentaron un ataque de denegación de

servicio que puede iniciarse sobrecargando un *«AP al iniciar una gran cantidad de apretones de manos con un punto de acceso habilitado para WPA3»*, omitiendo el mecanismo anti-obstrucción de SAR que se supone evita los ataques DoS.

Algunas de estas vulnerabilidades también afectan a los dispositivos que utilizan el protocolo EAP-pwd (Protocolo de autenticación extensible-contraseña), que también se basa en el método de intercambio de claves autenticado con contraseña de Dragonfly.

Como prueba de concepto, los investigadores lanzarán en breve las siguientes cuatro herramientas separadas (en los repositorios de GitHub con un enlace a continuación) que pueden usarse para probar las vulnerabilidades como se mencionó anteriormente.

- Dragondrain: Una herramienta que puede probar hasta qué punto un punto de acceso es vulnerable a los ataques DoS contra el saludo de la libélula de WPA3.
- Dragontime: Una herramienta experimental para realizar ataques de tiempo contra el saludo de Dragonfly.
- Dragonforce: Una herramienta experimental que toma la información para recuperarse de los ataques de tiempo y realiza un ataque de partición de contraseñas.
- Dragonslayer: Una herramienta que implementa ataques contra EAP-pwd.

> *«Casi todos nuestros ataques son contra el método de codificación de contraseña de SAE, es decir, contra su algoritmo hash-to-group y hash-to-group. Curiosamente, un simple cambio de este algoritmo habría evitado la mayoría de nuestros ataques»*, agregaron.

WiFi Alliance trabaja con los proveedores para solucionar los

problemas informados

El dúo de investigadores informó sobre sus hallazgos a WiFi Alliance, la organización sin fines de lucro que certifica los estándares de WiFi y los productos de WiFi para la conformidad. Dicha organización reconoció los problemas y está trabajando con los proveedores para parchear los dispositivos con certificación WPA3 existentes.

> *«Las actualizaciones de software no requieren ningún cambio que afecte la interoperabilidad entre los dispositivos WiFi. Los usuarios pueden consultar los sitios web de los proveedores de sus dispositivos para obtener más información»* dice WiFi Alliance en un comunicado de prensa.

Puedes leer más acerca de estas vulnerabilidades en el sitio web dedicado de DragonBlood y en el documento de investigación, que también explicar cómo pequeños cambios en el protocolo podrían prevenir la mayoría de los ataques detallados por los investigadores.