Un equipo de investigadores de seguridad cibernética, mismo que descubrió las graves vulnerabilidades Dragonblood en el estándar de seguridad WiFi WPA3, ahora descubrió dos fallas más que podrían permitir a los atacantes piratear contraseñas de WiFi.

WPA o WiFi Protected Access, es un estándar de seguridad WiFi que fue diseñado para autenticar dispositivos inalámbricos mediante el protocolo del Estándar de Cifrado Avanzado (AES), y está destinado a evitar que los piratas informáticos accedan a los datos de la red.

El protocolo WiFi Protected Access III (WPA3), se lanzó hace un año en un intento por abordar las deficiencias técnicas del protocolo WPA2, que por mucho tiempo se consideró inseguro y vulnerable a ataques KRACK más graves.

WPA3 se basa en un acuerdo denominado SAE (Autenticación Simultánea de Iguales), que también se conoce como Dragonfly, y tiene como objetivo la protección de redes WiFi contra ataques de diccionario fuera de línea.

Sin embargo, en menos de un año, los investigadores de seguridad Mathy Vanhoef y Eyal Ronen, encontraron varias debilidades (Dragonblood) en la implementación temprana de WPA3, permitiendo que un atacante recupere las contraseñas de WiFi al abusar del tiempo o las fugas de canal lateral basadas en caché.

Poco después de esa divulgación, WiFi Alliance, la organización sin fines de lucro que supervisa la adopción del estándar WiFi, lanzó parches para abordar los problemas y creó recomendaciones de seguridad para mitigar los ataques iniciales de Dragonblood.

Pero dichas recomendaciones de seguridad, que fueron creadas de forma privada sin colaboración con los investigadores, no son suficientes para proteger a los usuarios contra los ataques de Dragonblood. En cambio, abre dos nuevos ataques de canal lateral, que una vez más permite a los hackers robar las contraseñas WiFi aún si se utiliza la última versión del protocolo WiFi.

Nuevo ataque de canal lateral contra WPA3 cuando se utilizan curvas Brainpool

La primera vulnerabilidad, identificada como CVE-2019-13377, es un ataque de canal lateral basado en el tiempo contra el apretón de manos Dragonfly de WPA3 cuando se utilizan las curvas de Brainpool, que la Alianza WiFi recomendó a los proveedores usar como una de las recomendaciones de seguridad para agregar otra capa de seguridad.

> *«Sin embargo, descubrimos que el uso de las curvas de Brainpool introduce la segunda clase de fugas de canal lateral en el apretón de manos Dragonfly de WPA3. En otras palabras, incluso si se siguen los consejos de WiFi Alliance, las implementaciones siguen en riesgo de ataques»,* dicen los investigadores.

> *«La nueva fuga de canal lateral se encuentra en el algoritmo de codificación de contraseña Dragonfly, confirmamos la nueva fuga de Brainpool en la práctica contra la última versión de Hostapd, y pudimos forzar la contraseña con fuerza bruta utilizando la información filtrada»,* agregaron.

Ataque de canal lateral contra la implementación EAP-PWD de FreeRADIOUS

La segunda vulnerabilidad, identificada como CVE-2019-13456, es un error de fuga de información que reside en la implementación de EAP-pwd (Protocolo de autenticación de contraseña extensible), en FreeRADIOUS, uno de los servidores RADIOUS de código abierto más utilizados que las empresas usan como una base de datos central para autenticar usuarios remotos.

Mathy Vanhoef, uno de los dos investigadores que descubrió las fallas de Dragonblood, dijo a THN que un atacante podría iniciar varios EAP-pwd para filtrar información, que luego se puede usar para recuperar la contraseña WiFi del usuario mediante la realización de

diccionario y fuerza bruta.

> *«El protocolo EAP-pwd utiliza internamente Dragonfly, y este protocolo se usa en algunas redes empresariales donde los usuarios se autentican mediante un nombre de usuario y contraseña»,* dijo Vanhoef.
>
> *«Más preocupante, encontramos que el firmware WiFi de los chips Cypress solo ejecuta 8 iteraciones como mínimo para evitar fugas en los canales laterales. Aunque esto hace que los ataques sean más difíciles, no los evita»*, agregó.

Según los investigadores, la implementación del algoritmo Dragonfly y WPA3 sin fugas de canal lateral es sorprendentemente difícil, y las contramedidas compatibles con estos ataques son demasiado costosas para dispositivos livianos.

Los investigadores compartieron sus nuevos hallazgos con WiFi Alliance y tuitearon que *«el estándar WiFi ahora se está actualizando con las defensas adecuadas, lo que podría conducir a WPA 3.1»*, pero desafortunadamente, las nuevas defensas no serían compatibles con la versión inicial de WPA3.

Mathy Vanhoef también informó que es lamentable que WiFi Alliance hata creado sus pautas de seguridad en privado. *«Si hubieran hecho esto públicamente, estos nuevos problemas podrían haberse evitado. Incluso la certificación WPA3 original se hizo en parte en privado, lo que tampoco fue ideal».*