Các nhà nghiên c□u v□a ti□t l□ m□t s□ l□ h□ng nghiêm tr□ng trong giao th□c b□o m□t không dây có th□ cho phép k□ t□n công l□y đ□□c m□t kh□u c□a m□ng Wi-Fi.

"WPA" là vi□t t□t c□a Wi-Fi Protected Access, m□t giao th□c b□o m□t cho m□ng Wi-Fi. Giao th□c Wi-Fi Protected Access III (WPA3) đã đ□□c đ□a ra trong n□ l□c gi□i quy□t các thi□u sót k□ thu□t c□a giao th□c WPA2, t□ lâu đã đ□□c coi là không an toàn và d□ b□ KRACK (T□n công cài đ□t l□i khóa).

WPA3 đ□□c gi□i thi□u s□ mang l□i s□ b□o v□ m□nh m□ ngay c□ khi ng□□i dùng ch□n m□t kh□u ng□n và không ph□c t□p. Nói cách khác, ngay c□ khi b□n đang s□ d□ng m□t m□t kh□u y□u, tiêu chu□n WPA3 s□ b□o v□ ch□ng l□i các cu□c t□n công brute-force. Đây là ki□u t□n công mà m□t máy khách c□ g□ng đoán m□t kh□u, hành đ□ng này l□p đi l□p l□i cho đ□n khi nó tìm đ□□c m□t kh□u chính xác. Mathy Vanhoef, nhà nghiên c□u b□o m□t đã phát hi□n ra KRACK, t□ ra r□t thích v□ nh□ng c□i ti□n b□o m□t trong WPA3.

Tuy nhiên, có v□ nh□ công ngh□ nào cũng có nhi□u l□ h□ng, và WPA3 cũng v□y. M□c dù WPA3 d□a vào m□t giao th□c k□t n□i-giao ti□p an toàn h□n, đ□□c g□i là Dragonfly nh□m b□o v□ các m□ng Wi-Fi ch□ng l□i các cu□c t□n công ngo□i tuy□n.

Các nhà nghiên c□u b□o m□t Mathy Vanhoef và Eyal Ronen đã tìm th□y đi□m y□u trong vi□c tri□n khai s□m WPA3-Personal, cho phép k□ t□n công khôi ph□c m□t kh□u Wi-Fi d□ dàng b□ng cách s□ d□ng k□ thu□t liên quan đ□n abusing timing (mã l□i CVE-2019-9494) ho□c l□y đ□□c cache-based side-channel (mã l□i CVE-2019-9494).

C□ th□, nh□ng k□ t□n công có th□ đ□□c thông tin WPA3 đ□□c cho là mã hóa an toàn. Đi□u này có th□ b□ l□m d□ng đ□ đánh c□p thông tin nh□y c□m nh□ s□ th□ tín d□ng, m□t kh□u, tin nh□n trò chuy□n, email,...

Đ□ t□n công phân vùng l□u tr□ m□t kh□u, chúng tôi c□n ghi l□i m□t s□ l□n liên k□t v□i các đ□a ch□ MAC khác nhau. Chúng tôi có th□ k□t n□i v□i các đ□a ch□ MAC khác nhau b□ng cách nh□m m□c tiêu nhi□u khách hàng trong cùng m□t m□ng (ví d□: thuy□t ph□c nhi□u ng□□i dùng t□i xu□ng cùng m□t □ng d□ng đ□c h□i). Ho□c tr□□ng h□p ch□ có th□ t□n công m□t thi□t b□, chúng tôi có th□ thi□t l□p các tr□m l□a đ□o có cùng SSID nh□ng đ□a ch□ MAC gi□ m□o - hai nhà nghiên c□u cho bi□t.

Bên c□nh đó, nghiên c□u cũng ghi nh□n m□t cu□c t□n công t□ ch□i d□ch v□ (DoS) có th□ đ□□c kh□i ch□y b□ng cách kh□i đ□ng m□t s□ l□□ng l□n các k□t n□i v□i Access Point h□ tr□ WPA3, b□ qua c□ ch□ ch□ng t□c ngh□n c□a SAE đ□□c cho là đ□ ngăn ch□n các cu□c t□n công DoS.

Hi□n t□i nghiên c□u này đã đ□□c báo cáo cho WiFi Alliance, t□ ch□c phi l□i nhu□n ch□ng nh□n các tiêu chu□n WiFi và các s□n ph□m Wi-Fi phù h□p. H□ đã th□a nh□n các v□n đ□ và đang làm vi□c v□i các nhà cung c□p đ□ vá các thi□t b□ đ□□c ch□ng nh□n WPA3 hi□n có.

(VNN)