Ecco Dragonblood, la prima vulnerabilità di WPA3

Apr 11, 2019 Marco Schiaffino In evidenza, News, RSS, Tecnologia, Vulnerabilità 0

Il nuovo standard non è ancora entrato a regime ma spunta già una falla di sicurezza che consente di violare il sistema di autenticazione.

Niente panico: per una volta, la vulnerabilità è spuntata esattamente quando doveva farlo, cioè quando i dispositivi che implementano lo standard sono pochi e vengono costantemente monitorati per verificare se spuntano eventuali problemi.

A specificarlo è la stessa **Wi-Fi Alliance**, nel comunicato stampa che ha pubblicato per segnalare la scoperta di **Dragonblood**, una falla di sicurezza che affligge il nuovo protocollo **WPA3-Personal**.

I problemi nascono dal fatto che il nuovo sistema di handshacking, noto come **Simultaneous Authentication of Equals (SAE)** o **Dragonfly**, permetterebbe di raccogliere informazioni attraverso un attacco side-channel, oltre a "non implementare in maniera appropriata alcune operazioni crittografiche o usare componenti di crittografia indesiderati".

Insomma: come spiegano **Mathy Vanhoef** ed **Eyal Ronen**, i due ricercatori che hanno scoperto la falla di sicurezza, si apre la possibilità che un pirata informatico possa violare la password di autenticazione attraverso una serie di azioni combinate.

Un attacco che permetterebbe di intercettare informazioni riservate come numeri di carte di credito, password, messaggi

di chat, email e simili.

I due ricercatori hanno anche pubblicato su Internet una serie di tools che dimostrano l'efficacia delle tecniche di attacco, che si muovono su due binari.

Alcune sfruttano un sistema di **downgrade**, forzando in pratica il dispositivo ad "abbandonare" WPA3 per utilizzare WPA2, che utilizza il vecchio sistema di scambio di informazioni.

Queste ultime possono essere utilizzate per effettuare un attacco a dizionario offline che permetterebbe di violare il sistema di autenticazione del dispositivo.

Una variante di questo attacco, che i ricercatori definiscono "downgrade di gruppo", prevede un attacco di jamming in grado di "ingannare" i dispositivi collegati alla rete Wi-Fi e **forzarli a utilizzare i protocolli di crittografia più deboli di quelli normalmente utilizzati**.

Il secondo binario è rappresentato dagli attacchi side-channel, sia di tipo cache che di tipo timing, che consentirebbero di recuperare la password attraverso una tecnica simile all'attacco a dizionario (**password partitioning**).

Vanhoef e Ronen, spiegano nel loro report, non hanno pubblicato tutti i dettagli delle vulnerabilità che hanno individuato e stanno collaborando con la Wi-Fi Alliance e i produttori per risolvere quelli ancora "aperti". Per tutti gli

altri sarebbero già state realizzate le patch che correggono lo standard.

Please follow and like us:

Password predefinita nell’app: migliaia di auto a rischio furto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/11/ecco-dragonblood-la-prima-vulnerabilita-di-wpa3/