Router 4G a rischio attacco. Avete aggiornato il firmware?

Ago 13, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Una raffica di bug individuata nei modelli più diffusi consentirebbe a un pirata informatico di rubare informazioni e portare attacchi al dispositivo.

A ben vedere, l'allarme lanciato riguardo le vulnerabilità dei **router 4G** rappresenta un clamoroso paradosso. I dispositivi che consentono il collegamento a Internet in mobilità, infatti, sono usati per lo più da chi ha a cuore la sicurezza e preferisce portarsi con sé una rete Wi-Fi di "proprietà" piuttosto che usare i vari hotspot gratuiti.

Stando a quanto spiegano in un report i ricercatori di **Pen Test Partners**, però, questo tipo di dispositivi soffre di numerose falle di sicurezza che rischiano di esporre gli utenti al rischio di attacchi e furti di informazioni. Peggio ancora: i produttori sembrano preoccuparsi ben poco dei rischi individuati dai ricercatori.

I router 4G sono, essenzialmente, molto simili ai router domestici, con una semplice differenza: al posto di collegarsi a una linea fissa, utilizzano una SIM dati per garantire la connessione.

Il problema è che con l'introduzione di funzionalità hotspot per le SIM in dotazione ai normali smartphone (la disponibilità della funzione dipende dall'operatore) i router 4G hanno perso un po' di appeal sul mercato. **Come se non bastasse, il prossimo passaggio al 5G viene visto dai produttori come un passaggio che renderà obsoleti gli attuali**

modelli.

Risultato: secondo Pen Test Partners stiamo assistendo a una pericolosa inerzia nell'aggiornamento dei software di controllo dei dispositivi. Un'ipotesi confermata dal racconto che i ricercatori fanno delle procedure di disclosure avviate con vari produttori.

Partiamo da **ZTE**, i cui router **MF910** sono finiti sotto la lente di ingrandimento dei ricercatori. Le vulnerabilità individuate in questo caso sono due: la prima (CVE-2019-3411) riguarda un leak di informazioni (la password di amministrazione) mentre la seconda (CVE-2019-3412) consentirebbe di iniettare comandi e, di conseguenza, **avviare l'esecuzione di codice in remoto**.

Quando i dettagli dei bug sono stati comunicati, il produttore ha però deciso di non correggerli. Motivo? Il prodotto sarebbe arrivato "a fine vita". Peccato che, come fanno notare dalle parti di Pen Test Partners, i router M910 sono ancora in vendita su numerosi siti come **Amazon**.

Tanto più che i ricercatori hanno trovato gli stessi problemi anche sul modello MF920, per il quale il supporto è ancora attivo. **Niente da fare: ZTE ha corretto il firmware solo per MF920 e il "vecchio" router rimane vulnerabile**.



L’altro produttore citato nel report è **Netgear**, il cui router **Nighthawk M1** sarebbe affetto da due falle di sicurezza che, ancora una volta, potrebbero portare a un attacco che consentirebbe l’esecuzione di codice in remoto.

Il primo problema riguarda una vulnerabilità (CVE-2019-14526) descritta come un “Cross-Site Request Forgery Protection Bypass” e che consentirebbe di **violare il sistema di protezione attraverso l’uso di un JavaScript inserito in una qualsiasi pagina Web**.

Il secondo, registrato come CVE-2019-14527, è relativo a un bug che consente a qualsiasi utente connesso di eseguire comandi attraverso l’interfaccia Web per la gestione del dispositivo.

In questo caso, spiegano gli analisti di Pen Test Partners, il produttore non ha risposto alla segnalazione inviata 5 mesi fa.

Insomma: il panorama nel settore dei router 4G è decisamente preoccupante e lo diventa ancora di più in vista del passaggio

al 5G, che potrebbe coincidere con un “rilancio” dei router mobili. Se le cose continuano così, ci aspettano tempi duri…

Condividi l’articolo

Attacco ransomware a una fotocamera? Si può fare!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/13/router-4g-a-rischio-attacco-avete-aggiornato-il-firmware/