QualPwn: come ti infetto lo smartphone Android dal Wi-Fi

Ago 06, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'uso combinato di due vulnerabilità permette di prendere il controllo di qualsiasi dispositivo Android equipaggiato con chip Qualcomm.

È stato battezzata **QualPwn** ed è probabilmente la tecnica di attacco più devastante mai messa a punto per colpire i dispositivi **Android**. L'anello debole della catena, in questo caso, sono i chip **Qualcomm Snapdragon**. Più precisamente, il componente dedicato al collegamento Wi-Fi.

Le falle di sicurezza, individuate dai ricercatori del **Tencent's Blade team** (qui la pagina Internet dedicata) permettono in pratica di violare qualsiasi sistema Android semplicemente attraverso l'invio di dati via Wi-Fi.

Nel dettaglio, la prima vulnerabilità (CVE-2019-10540) affligge il firmware equipaggiato sul controller Wi-Fi dei chip Qualcomm e consente di provocare un buffer overflow semplicemente inviando dei pacchetti che contengono il codice malevolo, che viene eseguito dal controller.

Già da sola, questa falla di sicurezza consentirebbe di installare un malware o uno spyware sul dispositivo senza che sia necessaria alcuna interazione da parte della vittima. L'unica condizione necessaria è che il pirata informatico sia collegato alla stessa rete Wi-Fi.

Le cose peggiorano, però, se i cyber-criminali utilizzano una seconda vulnerabilità (CVE-2019-10538) che permette di eseguire un passaggio fondamentale dal controller Wi-Fi al kernel Linux del chip Qualcomm. **In questo caso, infatti, sarebbero in grado di prendere il completo controllo del sistema**.

Ma quali sono i dispositivi vulnerabili? I ricercatori del Tencent's Blade team spiegano di aver testato l'attacco soltanto sui **Google Pixel2 e Pixel3**. A loro giudizio, però, dovrebbe funzionare su qualsiasi smartphone o tablet che equipaggia **Snapdragon 835 e 845**.

Ora il problema riguarda gli aggiornamenti. Per i dispositivi Google e (si spera) per buona parte dei maggiori produttori non c'è nessun problema, visto che Qualcomm ha reso disponibili gli aggiornamenti per il suo kernel già lo scorso giugno. **Rimane il problema di tutti quei dispositivi che, per**

motivi di età, non ricevono più aggiornamenti.

Se a questo aggiungiamo l’esercito di utenti che continua stolidamente a ignorare gli aggiornamenti, il rischio è che là fuori ci siano milioni di dispositivi Android a rischio attacco. La buona notizia è che, almeno per il momento, non è circolato alcun exploit pronto da usare. Incrociamo le dita…

Condividi l’articolo

Il 90% degli iPhone vulnerabili a un attacco via iMessage

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/06/qualpwn-come-ti-infetto-lo-smartphone-android-dal-wi-fi/