Apple suona l'allarme

Installate gli aggiornamenti software sui vostri prodotti Apple. È l’avvertimento lanciato direttamente dalla compagnia, dopo la scoperta nei giorni scorsi di una vulnerabilità in alcuni degli hardware sviluppati dalla società di Cupertino: un varco (tecnicamente un bug) che un hacker con intenzioni truffaldine potrebbe sfruttare per prendere il controllo di questi dispositivi e disporre dei dati. Gli aggiornamenti (o patch) sono stati rilasciati negli scorsi giorni e promettono di risolvere il problema.
Le falle (tecnicamente si tratta di vulnerabilità software cosiddette zero-day, ovvero non note agli sviluppatori, quindi particolarmente pericolose) sarebbero due: una riguarda il kernel, “lo strato più profondo del sistema operativo che tutti i dispositivi hanno in comune”, ha spiegato Cupertino.
L’altra, invece, riguarda Safari e in particolare WebKit, la tecnologia su cui si basa il browser. La versione da installare per mettere i propri dispositivi in sicurezza è la 15.6.1 per iOS, e la 12.5.1 per MacOs Monterey. Ad essere a rischio sono: tutti gli iPhone 6S e successivi (ovvero quelli rilasciati dal 2015 in avanti), tutti gli iPad dalla quinta generazione in avanti (ovvero rilasciati dal 2014), inclusi gli iPad Pro e tutti i Mac con a bordo Monterey.
Le vulnerabilità zero-day sono molto richieste sul mercato e valgono un sacco di soldi: proprio perché non sono note agli sviluppatori del software e permettono di sferrare attacchi in pratica senza che la vittima possa difendersi. Con le due scoperte ad agosto l’azienda di Cupertino ha risolto sette vulnerabilità zero-day dall’inizio dell’anno.

"Siamo a conoscenza di un report secondo cui questo problema potrebbe essere stato attivamente sfruttato” ha comunicato la società. Apple però non ha rivelato se ha informazioni sull'eventuale modo in cui il problema è stato sfruttato, la vulnerabilità sembra essere stata scoperta da un ricercatore anonimo.
Il bug consentirebbe agli intrusi di impersonare il proprietario del dispositivo e successivamente eseguire qualsiasi software a suo nome, ha dichiarato Rachel Tobac, Ceo di SocialProof Security, società che si occupa di sicurezza informatica, come riportato dal Guardian.
Quelli che dovrebbero prestare particolare attenzione all'aggiornamento del proprio software sono "persone che sono sotto gli occhi del pubblico", come attivisti o giornalisti che potrebbero essere il bersaglio di sofisticati spionaggio degli stati-nazione, ha aggiunto Tobac al quotidiano.