Il chip di sicurezza T2 di Apple a rischio attacco?

Ott 06, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'allarme circola in rete da qualche giorno e riguarda un attacco che permetterebbe di eseguire un jailbreak del co-processore. A rischio la sicurezza di macOS.

Per il momento gli esperti di sicurezza non si sbilanciano sull'applicabilità della tecnica di attacco, ma se dovesse essere confermata potrebbe trattarsi di una vera mazzata per la sicurezza dei computer **Apple**.

A finire nel mirino, infatti, è il chip di sicurezza **T2**, il co-processore che viene montato su tutti i computer con sistema **macOS** e a cui sono affidati, oltre alla gestione di alcuni servizi a basso livello, anche la gestione di dati sensibili come le chiavi crittografiche, le password di **Accesso Portachiavi**, il riconoscimento del Touch ID e la crittografia dei dischi.

Il chip T2 è stato introdotto nel 2017 e rappresenta uno dei classici strumenti di security basati sull'hardware. L'idea, in pratica, è quella di confinare tutti i dati sensibili in un chip distinto dal processore centrale er poterli proteggere meglio.

La comparsa di una vulnerabilità in grado di eseguire codice all'interno del chip T2 (qui è possibile leggere un report a riguardo pubblicato da **ironPeak**) di conseguenza ha immediatamente messo in allarme buona parte del mondo della sicurezza informatica.

Ma come funzionerebbe l’attacco? In pratica, sfrutterebbe due exploit ideati per il jailbreak dei sistemi **iOS**. Le due tecniche, chiamate **Checkm8** e **Blackbird**, deriverebbero la loro efficacia dal fatto che alcuni componenti hardware del chip sarebbero uguali a quelli usati nell’**iPhone**.

L’attacco, in ogni caso, richiede un accesso fisico al computer e in particolare un collegamento attraverso un cavo USB-C nella fase di avvio del computer utilizzando **Checkra1n** versione 0.11.0, un software per il jailbreaking piuttosto conosciuto.

Insomma: qualcosa che esclude (almeno per il momento) la possibilità di attacchi in remoto ma che apre la strada a tecniche di attacco hardware, spesso utilizzate da servizi segreti e gruppi APT.

Secondo i ricercatori, infatti, sarebbe possibile implementare l’attacco in modo che si avvii automaticamente al momento della connessione di un dispositivo o di un semplice cavo USB-C modificato ad arte per eseguire il jailbreak.

A rendere più spinosa la questione, c’è il fatto che la vulnerabilità non potrebbe essere corretta tramite un semplice aggiornamento, ma richiederebbe l’installazione ex novo di **BridgeOS**, il sistema operativo che gestisce il co-processore T2.

Condividi l’articolo

Invisibili per 9 anni: ESET accende i riflettori sul gruppo XDSpy

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/06/il-chip-di-sicurezza-t2-di-apple-a-rischio-attacco/?utm_source=rss&utm_medium=rss&utm_campaign=il-chip-di-sicurezza-t2-di-apple-a-rischio-attacco