Autogol di Xiaomi: il software di sicurezza ha una falla… di sicurezza

Apr 05, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug si nascondeva in Guard Provider, un'app preinstallata sui dispositivi Xiaomi. La vulnerabilità permette un attacco Man-in-the-Middle.

In ambiente **Android** ormai i maggiori problemi sembrano derivare dalle applicazioni preinstallate sui dispositivi. Succede nel caso degli attacchi che colpiscono la filiera di produzione (ne abbiamo parlato in questo articolo) ma anche per altri motivi.

Nel caso di **Xiaom**i, per esempio, la grana si è presentata sotto forma di una vulnerabilità in grado di consentire un attacco di tipo **Man-in-the-Middle (MiTM)** ai danni dei dispositivi del produttore cinese.

E non stiamo parlando di poca cosa: l'azienda con sede a Pechino, infatti, detiene **una quota di mercato dell'8% nel settore mobile, che ne fa il terzo produttore al mondo**. Stiamo parlando, quindi, di milioni di smartphone potenzialmente a rischio attacco.

Ma qual è esattamente il problema? Come spiegano i ricercatori di **Check Point**, che hanno individuato la falla e ne hanno descritto i dettagli in un report pubblicato su Internet, la vulnerabilità in questione si trova in un'applicazione di sicurezza preinstallata sui dispositivi Xiaomi.

Si chiama **Guard Provider** e avrebbe il compito di individuare eventuali malware, ma il bug nel suo codice avrebbe permesso a un eventuale pirata di portare l'attacco nel momento in cui si fosse trovato connesso alla stessa rete Wi-Fi.

All'origine del problema, secondo i ricercatori, c'è il fatto che l'applicazione è stata usata sfruttando troppi **SDK (Software Development Kit)** di terze parti che hanno portato, in buon sostanza, a un conflitto che ha messo a rischio gli utenti Xiaomi. In gergo questo fenomeno viene definito **SDK Fatigue**.

L'uso di questi kit di sviluppo, che per gli sviluppatori rappresentano una pratica scorciatoia per inserire funzionalità senza dover scrivere troppo codice, ha infatti un rovescio della medaglia: utilizzando porzioni di codice che non sono state scritte per lavorare insieme, si rischia il patatrac.

In questo caso è andata tutto sommato bene, visto che in seguito alla segnalazione di Check Point il produttore ha potuto sviluppare e distribuire tempestivamente la patch che corregge la falla di sicurezza e non sono stati registrati tentativi di attacco che sfruttassero il bug. La prossima

volta, però, potrebbe finire peggio.

Please follow and like us:

Facebook: 540 milioni di profili “dimenticati” su un server aperto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/05/autogol-di-xiaomi-il-software-di-sicurezza-ha-una-falla-di-sicurezza/