Password predefinita nell’app: migliaia di auto a rischio furto

Apr 10, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Gli sviluppatori di MyCar avevano “dimenticato” delle credenziali di amministratore inserite nel codice. Un ladro avrebbe potuto usarle per rubare le auto.

Così “smart” da essere facilissime da rubare. Le cosiddette “auto connesse” incappano nell’ennesimo incidente di sicurezza legato a un problema software.

Questa volta a finire sul banco degli imputati è **MyCar**, un set che consente di controllare a distanza alcune funzionalità dell’auto attraverso la connessione 3G e che può essere installato su numerosi modelli di veicoli per renderli “smart”.

Il sistema, come si legge sul sito, consente di aprire l’auto, accendere il motore, localizzare il veicolo, controllare la temperatura e molto altro ancora. Tutto attraverso un’app disponibile per **iOS** e **Android**.

Peccato che nel codice dell’app ci fosse **il classico account nascosto con privilegi di amministratore** che ogni tanto gli sviluppatori hanno la pessima abitudine di “dimenticare” nelle applicazioni. Risultato: chiunque lo avesse individuato avrebbe potuto accedere all’account di qualsiasi utente.

Foto di Will Dormann via Twitter

Insomma: un ladro avrebbe potuto collegarsi al server abbinando l'app a qualsiasi account, localizzare l'auto, aprirla e addirittura accenderla.

Ad accorgersene (qui il report originale) sono stati i ricercatori della **Carnagie Mellon University**, che hanno tempestivamente notificato il problema a MyCar e consentito allo sviluppatore di correggere il problema.

L'account è stato rimosso nelle nuove versioni dell'app (3.4.24 per iOS, 4.1.2 per Android) e, soprattutto, dai server del sistema. In questo modo anche gli utenti che non hanno ancora eseguito l'aggiornamento non rischiano più il furto "smart" della loro auto.

Tutta la vicenda si inserisce in una nuova fase delle vulnerabilità per le smart card. Se i primi casi hanno riguardato infatti i sistemi sviluppati dai produttori automobilistici, adesso le maggiori preoccupazioni riguardano i produttori di accessori, come è successo nel caso di alcuni antifurti "intelligenti" qualche settimana fa.

E visto che la sbornia di automazione attraverso i controlli via smartphone non sembra destinata a ridursi in tempi brevi,

è probabile (purtroppo) che ci troveremo a parlare ancora di casi simili.

Please follow and like us:

Ecco Dragonblood, la prima vulnerabilità di WPA3 Crittografia a prova di violazione? La soluzione è EverCrypt

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/10/password-predefinita-nellapp-migliaia-di-auto-a-rischio-furto/