Microsoft trova una voragine di sicurezza in un driver Huawei

Mar 27, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il software di controllo della casa cinese consentiva a un utente senza privilegi di creare processi con privilegi di "super amministratore".

Forse non rappresentano una minaccia per la sicurezza nazionale come sostiene Donald Trump, di certo però i prodotti **Huawei** qualche problema ce l'hanno. Uno lo ha individuato **Microsoft**, che ha segnalato all'azienda cinese un pericoloso bug in uno dei suoi driver.

Il rilevamento di questa vulnerabilità, spiegano i ricercatori di Microsoft, è avvenuto grazie a una nuova funzione di monitoraggio chiamata **Microsoft Defender APT**, introdotta con la versione 1809 di Windows 10.

Da un punto di vista tecnico, infatti, la falla di sicurezza individuata nel driver Huawei funziona in maniera molto simile a **DoublePulsar**, uno dei tool di hacking utilizzati dalla **National Security Agency** e resi pubblici dal leak degli **Shadow Brokers** nell'estate del 2017.

L'exploit creato dagli 007 americani sfrutta infatti una tecnica che consente l'esecuzione di codice nel corso di una sessione **Windows** avviata da un utente senza privilegi di amministratore attraverso una tecnica piuttosto elaborata.

Il codice in questione viene iniettato all'interno di un

processo dotato di privilegi e la sua esecuzione viene poi “forzata” attraverso un **APC** (asynchronous procedure calls), una funzionalità di Windows che consente di interrompere un processo e modificarne la funzione per velocizzare alcuni tipi di operazioni.

Huawei, in pratica, ha creato un driver che usa la stessa tecnica. La funzione, in realtà, rappresenta una sorta di sistema di monitoraggio che controlla il funzionamento di un servizio integrato in **PC Manager**, il software di manutenzione del produttore cinese.

Nel caso in cui il servizio venga terminato per qualsiasi motivo, il driver prevede il suo riavvio attraverso l’iniezione in un altro processo e l’uso di un APC per richiamarlo.

Una scelta piuttosto curiosa, che **apre però la strada alla possibilità che questa procedura venga avviata da un malware**, che in questo modo potrebbe eseguire codice con privilegi di

amministratore sfruttando il driver di Huawei come “trampolino di lancio”.

Questo comportamento anomalo, però, è stato rilevato dal sistema di analisi euristica di Microsoft Defender APT. Dopo la segnalazione da parte di Microsoft, Huawei ha corretto i suoi driver attraverso **un aggiornamento distribuito a gennaio**. Chi ha eseguito l’update, di conseguenza, può considerarsi al sicuro.

Please follow and like us:

Hackerato l’update automatico di Asus: backdoor su migliaia di PC

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/27/microsoft-trova-una-voragine-di-sicurezza-in-un-driver-huawei/