Cisco corregge 27 bug, ma due router rimangono vulnerabili

Mar 28, 2019 Marco Schiaffino News, RSS, Vulnerabilità 0

Il colosso statunitense pubblica ancora una volta un round di aggiornamenti incompleto. A rischio i modelli RV320 e RV325 che restano senza patch.

Per **Cisco**, quella di rilasciare patch incomplete sembra davvero essere diventata una (pessima) abitudine che rischia di esasperare i suoi utenti.

L'ennesimo "aggiornamento a metà" è stato rilasciato mercoledì, quando l'azienda californiana ha pubblicato un avviso relativo a 27 vulnerabilità (19 delle quali considerate "elevate") dei suoi prodotti.

Buona parte degli aggiornamenti riguardano **Cisco IOS XE**, il sistema operativo che gestisce router, switch e controller dell'azienda. I bug relativi a IOS XE comprendono iniezione di comandi, escalation dei privilegi e denial of service.

I veri problemi, però, riguardano due falle di sicurezza (CVE-2019-1652 e CVE-2019-1653) relative a due router per aziende di Cisco: **RV320 e RV325**. Entrambe erano state rese pubbliche e teoricamente corrette con una patch a gennaio.

Le cose, però, sembrano non essere andate per il verso giusto. Nell'avviso pubblicato mercoledì, infatti, si legge che "**la correzione iniziale per queste vulnerabilità si sono rivelate incomplete**". Cisco starebbe lavorando per risolvere la situazione e comunicherà quando il codice corretto sarà disponibile.

Insomma: gli utenti che utilizzano i due router, dedicati al mondo della piccola impresa, rimangono esposti al rischio che qualcuno riesca a sfruttare le vulnerabilità e comprometterne i sistemi.

Le due vulnerabilità, se sfruttate in un eventuale attacco, consentirebbero di reperire informazioni sensibili dai sistemi e addirittura di inviare comandi in remoto aggirando il sistema di autenticazione. I dispositivi **Dual Gigabit WAN VPN** affetti dal bug sono quelli con firmware nelle versioni **1.4.2.15** e successive.

L'unica possibilità è quella di incrociare le dita e sperare

che gli sviluppatori di Cisco riescano a mettere a punto rapidamente la patch in grado di correggere definitivamente i problemi.

Non è la prima volta che Cisco ha problemi di questo tipo. Lo scorso settembre, per esempio, abbiamo riportato una situazione simile in cui molti utenti sono rimasti “appesi” aspettando il rilascio degli aggiornamenti.

Please follow and like us:

Microsoft trova una voragine di sicurezza in un driver Huawei

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/28/cisco-corregge-27-bug-ma-due-router-rimangono-vulnerabili/