Router Cisco sotto attacco. I pirati usano due exploit in remoto

Gen 28, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS, Vulnerabilità 0

Due vulnerabilità combinate permettono di compromettere i dispositivi di rete attraverso una tecnica di command injection.

Allarme rosso per chi utilizza i router **Cisco RV320 e RV325**. I dispositivi in questione, infatti, sono sotto il tiro incrociato di numerosi gruppi di hacker che stanno sfruttando una catena di vulnerabilità (CVE-2019-1652 e CVE-2019-1653) per attaccarli.

A scatenare l'attività dei cyber-criminali è stata la comparsa su Internet di alcuni **Proof of Concept (PoC)** che permettono di sfruttare i due bug per iniettare comandi nei sistemi dei router e prenderne il controllo.

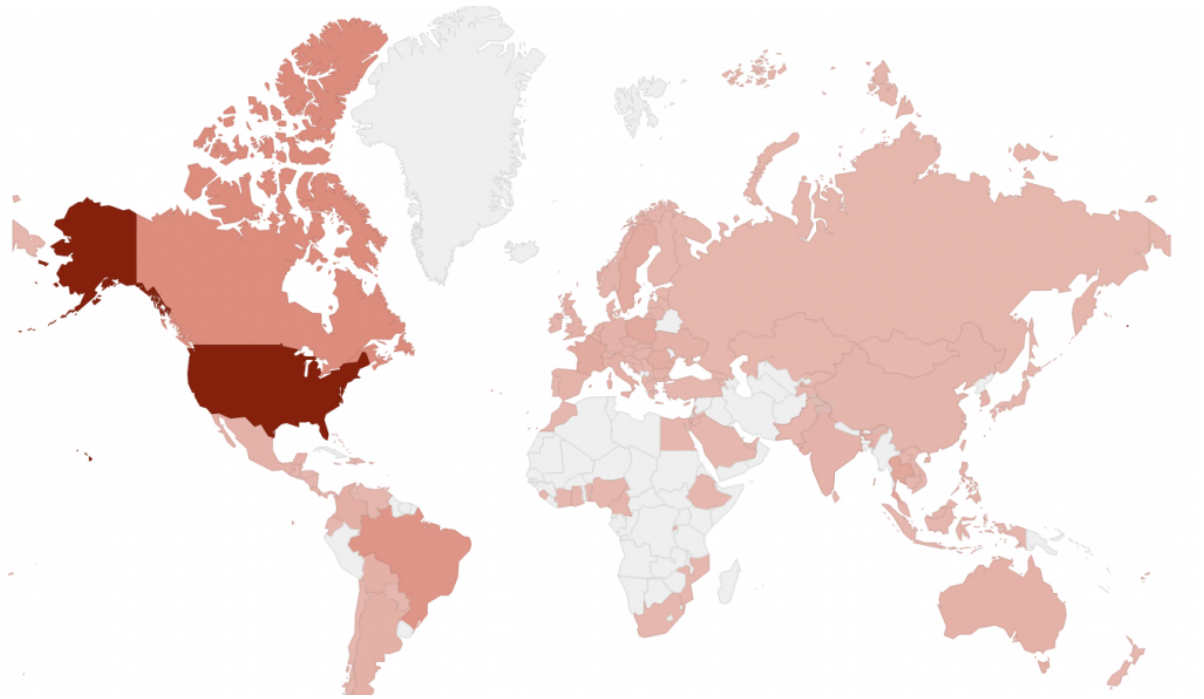
Nel dettaglio, la prima vulnerabilità (CVE-2019-1652) è quella che consente l'attacco **command injection**, ma per funzionare richiede che il pirata informatico operi come utente autenticato.

Qui entra in gioco la seconda falla di sicurezza (CVE-2019-1653) che permette di collegarsi in remoto ai router e ottenere le credenziali (sotto forma di hash) che permettono l'autenticazione.

L'uso combinato delle due vulnerabilità consente, in pratica, di collegarsi a un router, rubare le credenziali e utilizzarle

per inviargli comandi in remoto.

Su Internet risultano raggiungibili circa **20.000 router** RV320 e RV325, anche se una parte di questi potrebbe essere già stata aggiornata. Secondo la società di sicurezza **Bad Packets**, ci sarebbero **almeno 9.000 dispositivi vulnerabili**, la maggior parte dei quali si trova negli Stati Uniti.



Non si tratta di zero-day, ma di vulnerabilità scoperte dalla società tedesca **RedTeam Pentesting** e regolarmente comunicate a Cisco, che ha già rilasciato gli aggiornamenti che correggono i bug.

A rendere scottante la situazione, però, c'è il fatto che i modelli Cisco in questione sono dedicati al settore dello "small business", cioè installati in ambienti che difficilmente hanno policy di patching adeguate o un settore dedicato alla gestione della sicurezza, e che quindi rischiano di rimanere esposti per lunghi periodi di tempo prima che qualcuno si "accorga" del pericolo.

Please follow and like us:

Follow

Backdoor del governo russo in migliaia di siti Internet Bug in Microsoft Exchange e chiunque diventa amministratore

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/01/28/router-cisco-sotto-attacco-i-pirati-usano-due-exploit-in-remoto/