Attacchi attraverso uno zero-day ai firewall Sophos

Apr 27, 2020 Marco Schiaffino Attacchi, News, RSS, Vulnerabilità 0

La società di sicurezza ha dovuto pubblicare un aggiornamento di emergenza per bloccare gli attacchi al suo Sophos XG Firewall.

Intervento di emergenza per gli sviluppatori di **Sophos**, che nel corso degli ultimi giorni hanno dovuto fare gli straordinari per mettere mano al software che gestisce i firewall della serie XG.

Come si legge nella comunicazione pubblicata dall'azienda sul suo sito, i **Sophos XG Firewall** sono stati oggetto di una segnalazione riguardante una vulnerabilità relativa a una forma di **SQL injection** che metteva a rischio la sicurezza dei sistemi.

Un problema estremamente grave, la cui scoperta è arrivata solo quando un gruppo di hacker stava già utilizzando attivamente la vulnerabilità.

Attraverso la falla di sicurezza, era in pratica possibile estrarre dati dai dispositivi, ottenendo tutti gli username utilizzati localmente e gli hash delle password, con l'esclusione di quelle di **Active Directory** e **LDAP**.

I tecnici della società di sicurezza hanno sviluppato l'aggiornamento che corregge la vulnerabilità e lo hanno distribuito in modalità "push" per forzarne l'installazione su tutti i dispositivi. L'aggiornamento, spiegano dalle parti di Sophos, integra anche uno strumento che consente di verificare

se il dispositivo ha subito una compromissione o meno.

Nel caso in cui il sistema sia stato compromesso, si raccomanda di eseguire il reset degli account di amministrazione e riavviare il dispositivo. Non solo: i tecnici della società di sicurezza suggeriscono, come misura precauzionale, di eseguire il reset di tutti gli account degli utenti locali e delle password di tutti gli account che possono essere state utilizzate anche per le credenziali di accesso a XG.

Condividi l’articolo

Il ransomware Shade abbandona il campo. I pirati rilasciano le password Falla in Microsoft Teams: l’account si ruba con una GIF

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/27/attacchi-attraverso-uno-zero-day-ai-firewall-sophos/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-attraverso-uno-zero-day-ai-firewall-sophos