

SonicWall subisce un attacco che ha sfruttato una falla in un suo firewall

Gen 25, 2021 Marco Schiaffino Attacchi, In evidenza, Intrusione, News, RSS, Vulnerabilità 0

I pirati avrebbero sfruttato un bug zero-day presente nel dispositivo. L'azienda indaga e prepara la patch per correggere la vulnerabilità.

Subire un attacco informatico è piuttosto frustrante. Scoprire che i pirati hanno colpito grazie a una vulnerabilità zero-day presente in un tuo prodotto lo è probabilmente di più.

È quanto successo a **SonicWall**, azienda che produce dispositivi di rete tra cui VPN e Firewall. L'annuncio della violazione, pubblicato lo scorso venerdì attraverso uno scarno comunicato pubblicato sul sito dell'azienda, parla di un "attacco sofisticato" che avrebbe (probabilmente) sfruttato una falla di sicurezza sconosciuta, presente nelle stesse appliance di sicurezza SonicWall.

I prodotti individuati in un primo momento dall'azienda come possibili bersagli dell'attacco sono due: i clienti **NetExtender VPN** e i gateway **Secure Mobile Access (SMA)**.

Nell'aggiornamento pubblicato nella giornata di sabato, però, SonicWall ha specificato che il campo è stato ristretto ai **dispositivi SMA della serie 100**, escludendo che il problema possa trovarsi nel client VPN.

Mentre gli esperti di SonicWall continuano a investigare per definire i contorni e le dinamiche dell'attacco subito dall'azienda, i suoi tecnici si sono preoccupati di comunicare alcuni accorgimenti che permetterebbero di mitigare il rischio di attacchi per gli utenti che usano i due prodotti in questione.

Nel dettaglio, il loro suggerimento è di **limitare le connessioni ai dispositivi SMA attraverso la predisposizione di una White List che consenta di bloccare eventuali comunicazioni malevole**. Questo, spiegano nel comunicato, può essere fatto attraverso un firewall o utilizzando gli stessi sistemi di configurazione di SMA.

L'attacco a SonicWall conferma una nuova tendenza, emersa in queste ultime settimane, che vede evidentemente i pirati informatici particolarmente interessati agli strumenti e alle tecnologie in uso alle società di sicurezza. Prima dell'azienda californiana, infatti, a subire le "attenzioni" dei cyber criminali sono stati **FireEye, Microsoft e Malwarebytes**.

Condividi l'articolo

Rubano le credenziali a migliaia di utenti ma i dati finiscono su... Google!

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2021/01/25/sonicwall-subisce-un-attacco-che-ha-sfruttato-una-falla-in-un-suo-firewall/?utm_source=rss&utm_medium=rss&utm_campaign=sonicwall-subisce-un-attacco-che-ha-sfruttato-una-falla-in-un-suo-firewall