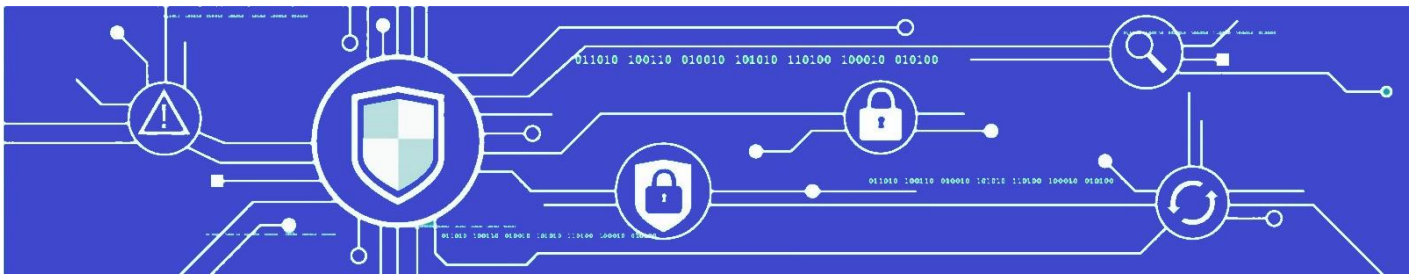

Vulnerabilità in SonicWall NetExtender (Windows)

La VPN SSL NetExtender di SonicWall consente agli utenti Windows di stabilire una connessione semplice e sicura tramite Internet alla rete di una struttura (centro di controllo), consentendo l'accesso remoto. È stata riscontrata una vulnerabilità nel client SonicWall NetExtender per Windows 10.2.337 e versioni precedenti. Il produttore ha fornito un aggiornamento del software VPN e consiglia vivamente agli utenti di aggiornare alla versione più recente del client NetExtender.

Di cosa si tratta?

SonicWall NetExtender Client per Windows 10.2.337 e versioni precedenti sono installati con il driver sfpmonitor.sys. Le applicazioni client comunicano con il driver tramite query. Il metodo del driver che gestisce queste query presenta una vulnerabilità di buffer overflow basata su stack che potrebbe consentire a un utente malintenzionato di creare una query specifica per sovrascrivere la memoria del kernel, causando un Denial of Service (DoS) che potrebbe potenzialmente portare all'esecuzione di codice nel sistema operativo di destinazione.

Vulnerabilità:
CVE-2023-6340
CVSS: Stack-based Buffer Overflow
Vulnerability: 8.2 (high)

Versione(e) fissa(e): NetExtender per Windows versione 10.2.338 (disponibile dal 16 gennaio 2024)

Qual è la situazione delle minacce nel mio sistema?

Questa vulnerabilità consente a un utente malintenzionato di prendere il controllo di un notebook o di un computer desktop e di eseguirvi codice dannoso. Esiste il rischio che il sistema di controllo possa essere infettato se qualcuno si connette ad esso. Si raccomanda di evitare operazioni da remoto fino a quando il client VPN non sarà stato aggiornato.

Sono interessate tutte le versioni di NetExtender Windows Client 10.2.337 (Windows 32 e 64 bit) e precedenti.

Questa vulnerabilità non comporta rischi per i sistemi operativi iOS e Android.
Tuttavia, si consiglia di mantenere tutti i sistemi aggiornati.

Occorre prestare particolare attenzione a quanto segue:
Fate attenzione a Windows 7: questo sistema operativo non è più supportato da Microsoft e dall'ultimo client NetExtender.

I computer gestiti da un reparto IT interno necessitano di un'autorizzazione corrispondente per installare l'ultima versione di NetExtender. A tal fine, si prega di contattare direttamente il proprio reparto IT interno .

Come posso proteggermi da questo fenomeno ?

L'ultima versione di NetExtender Client 10.2.338 può essere scaricata dal sito web del produttore. :

https://www.sonicwall.com/de-de/products/remote-access/vpn-clients/

Un video di istruzioni è stato salvato sul portale Vimeo:

https://player.vimeo.com/video/903647259?h=428c46b562

Per ricevere assistenza, è possibile chiamare la hotline a pagamento al numero **0844 11 22 11**. Se si usufruisce di un contratto di manutenzione con servizio di aggiornamento, i costi non vengono applicati.

Update Service
Ogni sistema deve essere aggiornato regolarmente per proteggerlo dalle nuove vulnerabilità scoperte. In particolare, consigliamo di aggiornare regolarmente il software dei firewall, che sono il componente di sicurezza più importante per la protezione della rete.

Con questo servizio, Rittmeyer controlla periodicamente la sicurezza, testa e installa gli aggiornamenti del software.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity