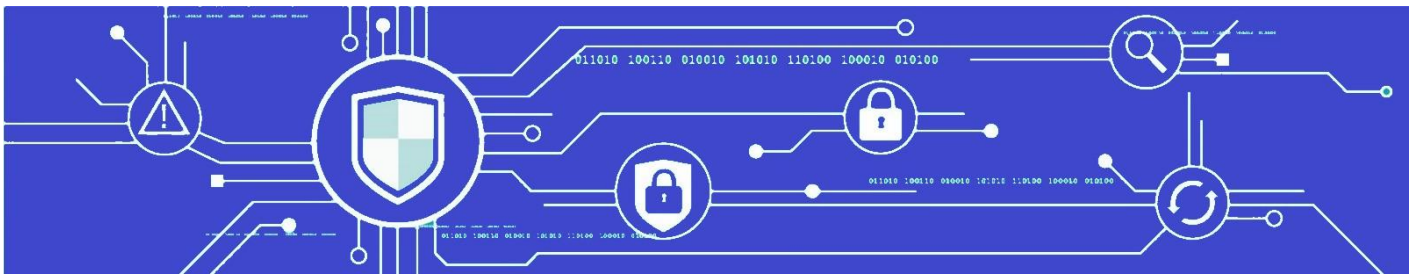

Schwachstelle in SonicWall NetExtender (Windows)

Mit dem SSL VPN NetExtender von SonicWall können Windows-Benutzer eine einfache und sichere Verbindung über das Internet zum Netzwerk einer Anlage (Leitstelle) herstellen und so einen Fernzugriff ermöglichen. Im SonicWall NetExtender Client für Windows 10.2.337 und frühere Versionen wurde eine Schwachstelle gefunden. Der Hersteller hat ein Update zum Aktualisieren der VPN-Software bereitgestellt und rät den Benutzern dringend, auf die neueste NetExtender Client Version upzudaten.

Um was geht es?

SonicWall NetExtender Client für Windows 10.2.337 und frühere Versionen werden mit dem Treiber sfpmonitor.sys installiert. Die Client-Anwendungen kommunizieren mit dem Treiber über Abfragen. Die Treibermethode, die diese Abfragen verarbeitet, weist eine stapelbasierte Pufferüberlaufschwachstelle auf, die es einem Angreifer ermöglicht, eine bestimmte Abfrage so zu gestalten, dass Kernelspeicher überschrieben wird, was zu einem Denial of Service (DoS) führt, der möglicherweise die Ausführung von Code im Zielbetriebssystem zur Folge hat.

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

Behobene Version(en): NetExtender für Windows Version **10.2.338** (verfügbar ab dem 16. Januar 2024)

Wie ist die Bedrohungslage auf meiner Anlage?

Diese Schwachstelle ermöglicht es einem Angreifer, die Kontrolle über einen Notebook oder Desktop Computer zu übernehmen und darauf Schadcode auszuführen. Es besteht die Gefahr, dass das Leitsystem infiziert wird, wenn sich jemand damit verbindet. Verzichten Sie auf Fernwartungen, bis der VPN-Client aktualisiert wurde.

Alle NetExtender Windows Client 10.2.337 (Windows 32 und 64 bit) und frühere Versionen sind betroffen.

Für die Betriebssysteme von iOS und Android besteht für diese Schwachstelle keine Gefahr. Wir empfehlen jedoch alle Systeme auf dem aktuellen Stand zu halten.

Folgendes gilt es besonders zu beachten:
Vorsicht bei Windows 7 – dieses Betriebssystem wird von Microsoft und vom neuesten NetExtender Client nicht mehr unterstützt.

Computer, welche von einer internen IT-Betrieben werden, brauchen dementsprechende Berechtigung zum Installieren des neuesten NetExtenders. Wenden sie sich dazu bitte direkt an ihre interne IT.

Wie kann ich mich dagegen schützen?

Der aktuelle NetExtender Client 10.2.338 kann von der Herstellerseite heruntergeladen werden:

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

Eine Anleitungsvideo wurde auf das Vimeo-Portal gespeichert:

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

Für Unterstützung können Sie sich kostenpflichtig an die Hotline unter **0844 11 22 11** wenden. Wenn Sie den Update-Service nutzen, entfallen die Kosten.

Update Service
Jedes System sollte regelmässig aktualisiert werden, um es gegen neu entdeckte Schwachstellen zu schützen. Gerade bei einer Firewall empfehlen wir Ihnen einen regelmässigen Software-Update, da es sich um die wichtigste Netzwerk-Sicherheits-Komponente zum Schutz ihres Netzwerkes handelt.

Mit dem Service übernimmt Rittmeyer periodisch die Kontrolle der Security, das Testen und Installieren der Software- Updates.

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