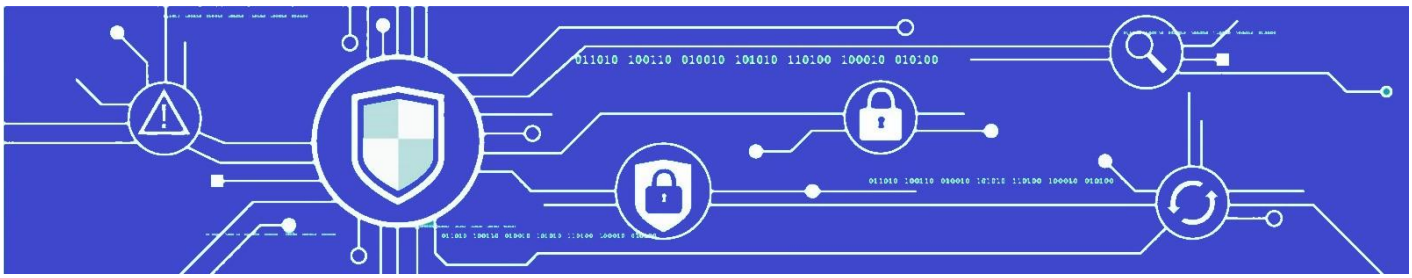


Vulnérabilité identifiée dans SonicWall NetExtender (Windows)

Le SSL VPN NetExtender de SonicWall permet aux utilisateurs de Windows d'établir une connexion à distance simple et sécurisée via Internet au réseau informatique de votre poste de commande. Une vulnérabilité a été découverte dans le client SonicWall NetExtender pour Windows 10.2.337 et les versions antérieures. Le fabricant a mis à disposition une mise à jour pour actualiser le logiciel VPN et conseille vivement aux utilisateurs de passer à la dernière version du NetExtender Client.

De quoi s'agit-il ?

SonicWall NetExtender Client pour Windows 10.2.337 et versions antérieures s'installe avec le pilote sfpmonitor.sys. Les applications clientes communiquent avec le pilote par le biais de requêtes. La méthode du pilote qui traite ces requêtes présente une vulnérabilité de dépassement de mémoire tampon basée sur la pile qui permet à un attaquant de concevoir une requête spécifique de manière à écraser la mémoire du noyau, ce qui entraîne un déni de service (DoS) et éventuellement l'exécution de code dans le système d'exploitation cible.

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

Version(s) corrigée(s) : NetExtender pour Windows version 10.2.338 (disponible à partir du 16 janvier 2024)

Quel est le niveau de menace sur mon installation ?

Cette vulnérabilité permet à un attaquant de prendre le contrôle d'un ordinateur portable ou de bureau et d'y exécuter un code malveillant. Il y a un risque d'infection du système de contrôle si quelqu'un s'y connecte. Renoncer à la maintenance à distance tant que le client VPN n'a pas été mis à jour.

Tous les clients Windows NetExtender 10.2.337 (Windows 32 et 64 bits) et les versions antérieures sont concernés.

Pour les systèmes d'exploitation iOS et Android, il n'y a aucun risque pour cette vulnérabilité.
Nous recommandons toutefois de maintenir tous les systèmes à jour.

Il convient d'accorder une attention particulière aux points suivants:
Attention à Windows 7 - ce système d'exploitation n'est plus pris en charge par Microsoft et par le dernier client NetExtender.

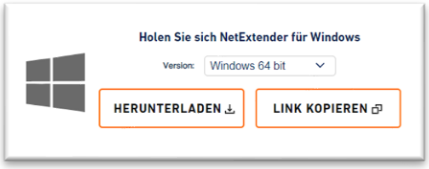
Les ordinateurs gérés par un service informatique interne doivent être autorisés à installer la dernière version de NetExtender. Dans ce cas, veuillez vous adresser directement à votre service informatique interne.

Comment se protéger ?

La dernière version du client NetExtender 10.2.338 peut être téléchargée sur le site du fabricant:

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

Cliquer ensuite sur "HERUNTERLADEN" pour télécharger le fichier :



Une vidéo pédagogique a été enregistrée sur le portail Vimeo : https://player.vimeo.com/video/903647259?h=428c46b562

Pour obtenir de l'aide, vous pouvez contacter la hotline au numéro payant suivant **0844 11 22 11**. Si vous souscrivez au service de mise à jour Rittmeyer, il n'y a pas de frais.

Service de mise à jour de Rittmeyer
Chaque système devrait être régulièrement mis à jour afin de le protéger contre les nouvelles vulnérabilités découvertes. Nous vous recommandons de mettre régulièrement à jour le logiciel du pare-feu, car il s'agit du composant de sécurité réseau le plus important pour la protection de votre réseau.

En choisissant le module de mise à jour, du contrat de maintenance, Rittmeyer se charge de contrôler périodiquement la sécurité, de tester et d'installer les mises à jour des logiciels de votre installation.

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