Vulnérabilité dans les pare-feux SonicWall avec SonicOS

Le fabricant SonicWall a publié un avis concernant une faille critique (CVE-2024-40766) dans le système d'exploitation SonicOS utilisé dans les pare-feux. Cette faille concerne notamment le composant SSLVPN et permet à des attaquants de faire planter le pare-feu et, dans certaines conditions, d'accéder à des ressources sensibles. SonicWall a déjà mis à disposition des mises à jour pour corriger cette faille et recommande de les installer immédiatement.

Um was geht es?

Une faille de sécurité critique affecte les pare-feux Sonicwall équipés du système d'exploitation SonicOS. Cette vulnérabilité concerne le contrôle d'accès ainsi que le composant SSLVPN. Dans certaines conditions, cela peut entraîner le plantage du pare-feu et un accès non autorisé aux ressources. Les appareils concernés sont ceux des séries Gen5, Gen6 et Gen7 avec des versions de firmware plus anciennes.

Détails de la vulnérabilité :

CVE CVE-2024-40766
CWE CWE-284: Improper Access Control
CVSS v3 9.3 (HIGH)
CVSS Vector
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:L

Selon le fabricant, les vulnérabilités ont été corrigées dans les versions suivantes :

5.9.2.14-13o (Gen5)
6.5.2.8-2n (für SM9800, NSsp 12400, NSsp 12800)
6.5.4.15.116n (Gen6)
Versions de firmware ultérieures à 7.0.1-5035 (Gen7)

Quelle est la situation de menace sur mon système ?

La faille permet à un attaquant de provoquer le plantage du pare-feu, ce qui peut affecter l'accès à distance, la gestion et le fonctionnement du système. De plus, il existe un risque que l'attaquant obtienne un accès non autorisé au pare-feu et se propage ensuite dans le réseau et sur d'autres systèmes. Cela peut entraîner des incidents de sécurité plus graves tels que la propagation de logiciels malveillants, le vol de données ou la manipulation de systèmes.

Comment puis-je m'en protéger ?

SonicWall a publié une mise à jour qui corrige cette faille.
Il est recommandé d'installer cette mise à jour dès que possible pour protéger vos systèmes.

Mettez à jour le firmware : Installez les mises à jour de firmware fournies par SonicWall pour corriger la vulnérabilité.

Changez les mots de passe : Modifiez les mots de passe des utilisateurs SSLVPN pour empêcher tout accès non autorisé.

Activez l'authentification multi-facteur : Renforcez la sécurité en activant l'authentification multi-facteur.

Pour obtenir de l'assistance, vous pouvez contacter notre hotline payante au 0844 11 22 11. Si vous utilisez notre service de mise à jour, ces frais seront supprimés.

Service de mise à jour
Chaque système doit être mis à jour régulièrement pour se protéger contre les vulnérabilités nouvellement découvertes. En particulier pour un pare-feu, nous recommandons des mises à jour logicielles régulières, car il s'agit du composant de sécurité réseau le plus important pour protéger votre réseau.
Avec le service de mise à jour, Rittmeyer assure périodiquement la vérification de la sécurité, le test et l'application des mises à jour logicielles.

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