GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPP 9108 Port-Vila, Vanuatu
Tel: (678) 33380

28 octobre 2025

Avis 99 : CVE-2024-40766 – Vulnérabilité dans le contrôle d'accès SonicOS
Date de publication : 10 septembre 2025
Degré d'impact : ÉLEVÉ/ CRITIQUE
TLP : CLAIR

CERT Vanuatu (CERTVU) et le service de Communication et de Transformation (SCTN) numérique publient la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

CERTVU a constaté une augmentation récente de l'exploitation active de cette vulnérabilité, qui est apparue en 2024 en tant que vulnérabilité critique dans les VPN SSL SonicWall.

Objet de l'alerte

Une vulnérabilité liée à un contrôle d'accès incorrect a été identifiée dans l'accès de gestion SonicOS et SSLVPN de SonicWall. Elle peut potentiellement entraîner un accès non autorisé aux ressources et, dans certaines conditions spécifiques, provoquer un arrêt du pare-feu.

Systèmes concernés

Cette vulnérabilité affecte les appareils SonicWall Gen 5 et Gen 6 ainsi que les appareils Gen 7 utilisant Sonic OS 7.0.1-5035 et les versions antérieures.

Les détails des versions affectées peuvent être consultés sur ce lien.

Implication

Les attaquants peuvent exploiter cette faille par les manières suivantes :

1. Accès non autorisé via des contrôles d'accès inappropriés – La vulnérabilité permet aux attaquants de contourner les contrôles d'accès et d'obtenir un accès non autorisé sans authentification.
2. Déploiement de logiciels rançonneurs (notamment Akira) – une fois à l'intérieur via un accès VPN SSL compromis, les attaquants – en particulier les complices du logiciels rançonneur Akira – utilisent ce point d'entrée pour lancer le logiciel rançonneur ou permettre l'extraction de données.

Mesures d'atténuation

1. Effectuez la mise à jour et appliquez le dernier correctif des versions affectées. Pour plus d'informations, veuillez consulter l'avis de sécurité CVE-2024.
2. Mise à jour du mot de passe pour les utilisateurs locaux – SonicWall recommande vivement à tous les utilisateurs de pare-feu Gen5 et Gen6 disposant de comptes SSLVPN gérés localement de mettre immédiatement à jour leur mot de passe afin de renforcer la sécurité et d'empêcher tout accès non autorisé.

Pour plus d'informations, consultez Gen7 et les pare-feux SonicWall les plus récents = activité malveillante SSLVPN.

Références

1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
2. cisa.gov/known-exploited-vulnerabilities-catalog