



BULLETIN DE SECURITE

Titre	Incidents de sécurité sur les pare-feux SonicWall Gen 7 avec SSLVPN
Numéro de Référence	56160508 /25
Date de Publication	05 Août 2025
Risque	Critique
Impact	Critique

Systemes affectés

- Pare-feux SonicWall Gen 7 avec SSLVPN activé

Bilan de la vulnérabilité

SonicWall déclare une hausse significative d'incidents de cybersécurité ciblant les pare-feux SonicWall Gen 7 avec « SSLVPN » activé. Une enquête est en cours pour déterminer s'il s'agit d'une vulnérabilité déjà connue ou d'une nouvelle faille (zero-day).

Solution

Dans l'attente de la publication d'un correctif, SonicWall recommande de :

- Désactiver SSLVPN si possible,
- Limiter l'accès SSLVPN à des IPs de confiance,
- Activer les services de sécurité intégrés (Botnet Protection, Geo-IP Filtering),
- Appliquer l'authentification multi-facteur (MFA), tout en notant que MFA seule peut ne pas suffire,
- Supprimer les comptes utilisateurs inutilisés, surtout ceux avec accès SSLVPN,
- Changements réguliers des mots de passe,

Risque

- Non spécifié

Annexe

Communiqué SonicWall du 04 août 2025:

- <https://www.sonicwall.com/support/notices/gen-7-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430>