ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits SonicWall
Numéro de Référence	58652111/25
Date de Publication	21 Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Gen7 hardware Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W,TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 version antérieure à 7.3.1-7013 ;
- Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) version antérieure à 7.3.1-7013 ;
- Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800 version antérieure à 8.0.3-8011 ;
- Email Security (ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V) version antérieure à 10.0.34.8215, 10.0.34.8223.

Identificateurs externes

- CVE-2025-32819, CVE-2025-32820, CVE-2025-32821

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits SonicWall susmentionnés.

- CVE-2025-40601, une faille de sécurité affectant SSLVPN SonicOS qui peut permettre aux attaquants de causer un déni de service sur les pare-feu vulnérables ;
- CVE-2025-40604 et CVE-2025-40605, deux vulnérabilités affectant les appliances de sécurité des emails, permettant aux attaquants distants de réussir une exécution de code arbitraire et d'accéder à des informations restreintes ;

Ces failles compromettent l'intégrité et la sécurité des appareils concernés. Il est fortement recommandé de mettre à jour les systèmes vers les versions corrigées.

Solution

Veuillez se référer au bulletin de sécurité SonicWall du 19 Novembre 2025 afin d'installer les nouvelles mises à jour.

Risque

- Déni de service ;
- Accès aux informations confidentielles ;
- Atteinte à la confidentialité des données ;
- Atteinte à l'intégrité des données ;
- Exécution du code arbitraire à distance.

Annexe

Bulletins de sécurité SonicWall du 19 Novembre 2025:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0016
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0018

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma