ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilité affectant SonicWall SONICOS IPSEC VPN
Numéro de Référence	48471907/24
Date de publication	19 Juillet 2024
Risque	Important
Impact	Important

Systèmes affectés

- SonicOS IPSec VPN Gen7 (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, NSv 270, NSv 470, NSv 870) versions 7.1.2-x antérieures à 7.1.2-7019
- SonicOS IPSec VPN Gen7 (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, NSv 270, NSv 470, NSv 870) versions 7.1.1-x antérieures à 7.1.1-7058
- SonicOS IPSec VPN Gen7 (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, NSv 270, NSv 470, NSv 870) versions 7.0.x antérieures à 7.0.1-5161
- SonicOS IPSec VPN Gen6 NSv (NSv10, NSv25, NSv50, NSv100, NSv200, NSv300, NSv400, NSv800, NSv1600) versions antérieures à 6.5.4.v-21s-RC2457

Identificateurs Externes

- CVE-2024-40764

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

SonicWall annonce la disponibilité d'une mise à jour de sécurité permettant de corriger une vulnérabilité affectant les versions susmentionnées de son produit SonicWall SONICOS IPSEC VPN. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant de causer un déni de service.

Solution

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

Risques

- Déni de service à distance

Références

Bulletin de sécurité de SonicWall :

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0012