



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans SonicWall SMA100 SSL-VPN
Numéro de Référence	51350512/24
Date de Publication	05 Décembre 2024
Risque	Critique
Impact	Critique

Systemes affectés

- SMA100 SSL-VPN Series (SMA 200, 210, 400, 410, 500v) versions antérieures à 10.2.1.14-75sv

Identificateurs externes

- CVE-2024-38475 CVE-2024-40763 CVE-2024-45318 CVE-2024-45319 CVE-2024-53702 CVE-2024-53703

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les versions susmentionnées de SonicWall SMA100 SSL-VPN. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service à distance et d'exécuter du code arbitraire à distance.

Solution

Veillez se référer au bulletin de sécurité SonicWall du 04 Décembre 2024 afin d'installer les nouvelles mises à jour.

Risque

- Déni de service à distance
- Exécution du code arbitraire à distance

Annexe

Bulletins de sécurité SonicWall du 04 Décembre 2024:

- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018>