AVIS DE SECURITE

Objet	**Multiples vulnérabilités dans Stormshield Network Security (SNS), dont une vérification de signature de mise à jour défaillante (CVE-2026-111090)**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-272
TLP	WHITE

Résumé

Stormshield a publié le 16/10/2026 plusieurs bulletins de sécurité concernant Stormshield Network Security (SNS). Deux d'entre eux portent sur une vérification de signature insuffisante des fichiers de mise à jour du pare-feu (STORM-2026-031, CVE-2026-111090, CVSS v3.1 7.8 ; STORM-2026-032, CVSS v3.1 7.5), pouvant permettre l'installation de fichiers de mise à jour non légitimes. D'autres bulletins signalent un XSS DOM dans le portail d'administration web (STORM-2026-022) et une faille de sévérité haute dont les détails sont encore sous embargo (STORM-2026-030). Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité
- Injection de code indirecte à distance (XSS)
- Exécution de code arbitraire (installation de mises à jour non authentifiées)

Systèmes affectés

- Stormshield Network Security (SNS) 5.1.x antérieures à 5.1.4 EA
- Stormshield Network Security (SNS) 5.0.x antérieures à 5.0.10
- Stormshield Network Security (SNS) 4.8.x antérieures à 4.8.20 LTSB
- Stormshield Network Security (SNS) 4.3.x jusqu'à 4.3.44 (CVE-2026-111090 / STORM-2026-031 et 032 ; aucun correctif indiqué pour cette branche : migrer vers une branche supportée)

Recommandations

Se référer aux bulletins de sécurité de l'éditeur du 16/10/2026 et appliquer les correctifs (SNS 5.1.4 EA, 5.0.10 ou 4.8.20 LTSB) :

- https://advisories.stormshield.eu/2026-022
- https://advisories.stormshield.eu/2026-030
- https://advisories.stormshield.eu/2026-031/
- https://advisories.stormshield.eu/2026-032/

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

E-mail : sncsirt@dcssi.sn

Date de publication : 23/10/2026