AVIS DE SECURITE

Objet	Vulnérabilité critique dans les produits de Fortinet
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2025-ADS-127
TLP	WHITE

Résumé

Une vulnérabilité critique exploitée depuis début 2023 vise certains produits Fortinet ayant activé la fonctionnalité SSL-VPN. Cette faille permet d'accéder à des données sensibles grâce à un lien symbolique installé après l'exploitation de vulnérabilités connues.

Risque de sécurité

- Accès au système compromis
- Vol de données
- Mouvement latéral

Systèmes affectés

FortiOS versions antérieures à :

- 7.0.17
- 7.2.11
- 7.4.7
- 7.6.2
- 6.4.16

Recommandations

- Mettre à jour FortiOS vers les versions corrigées publiées le 10 avril 2025
- En cas de compromission :
  - Isoler l'équipement touché,
  - Réinitialiser tous les secrets,
  - Rechercher des traces de persistance,
  - Faire une investigation.
- Se référer au bulletin suivant pour plus de détails : https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity