AVIS DE SECURITE

Objet	Vulnérabilités affectant des produits Splunk
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-255
TLP	WHITE

Résumé

Splunk annonce la correction de plusieurs vulnérabilités affectant ses produits mentionnés ci-après. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance, d'accéder à des données confidentielles, d'élever ses privilèges ou de causer un déni de service.

Risque de sécurité

- Exécution de code à distance
- Accès à des données confidentielles
- Elévation de privilèges
- Déni de service

Systèmes affectés

- Splunk Enterprise version 10.4.x antérieure à 10.4.3
- Splunk Enterprise version 10.2.x antérieure à 10.2.7
- Splunk Enterprise version 10.0.x antérieure à 10.0.10
- Splunk Enterprise version 9.4.x antérieure à 9.4.15
- Splunk Secure Gateway versions antérieures à 3.10.11, 3.9.25 et 3.8.72

Recommandations

Se référer aux Bulletins de sécurité de Splunk :

- https://advisory.splunk.com/advisories/SVD-2026-1001
- https://advisory.splunk.com/advisories/SVD-2026-1002