AVIS DE SECURITE

Objet	**Multiples vulnérabilités critiques dans Splunk Enterprise (SVD-2026-1007 et SVD-2026-1008)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-277
TLP	WHITE

Résumé

Splunk a publié le 21 octobre 2026 des mises à jour de sécurité pour Splunk Enterprise. L'avis SVD-2026-1008 corrige notamment deux vulnérabilités de contrôle d'accès et de neutralisation (CVE-2026-76299 et CVE-2026-76302) notées CVSS v3.1 9.9, ainsi que CVE-2026-76300 (8.8) ; l'avis SVD-2026-1007 corrige 12 vulnérabilités dont CVE-2026-76291 et CVE-2026-76298 (8.8) et CVE-2026-76293 (exécution de code à distance via Splunk Web, 7.2). Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Injection de code indirecte à distance (XSS) et falsification de requête (CSRF)

Systèmes affectés

- Splunk Enterprise 9.4.x antérieures à 9.4.16
- Splunk Enterprise 10.0.x antérieures à 10.0.11
- Splunk Enterprise 10.2.x antérieures à 10.2.8
- Splunk Enterprise 10.4.x antérieures à 10.4.4
- Splunk SOAR antérieur à 8.7.0 (avis SVD-2026-1010 à 1012)

Recommandations

Se référer aux bulletins de sécurité de l'éditeur du 21/10/2026 :

- https://advisory.splunk.com/advisories/SVD-2026-1008
- https://advisory.splunk.com/advisories/SVD-2026-1007
- https://advisory.splunk.com/advisories/SVD-2026-1009
- https://advisory.splunk.com/advisories/SVD-2026-1010