DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 19-06-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Splunk Enterprise
Réference	1486
Date de Publication	2026-06-19
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Compromission complète du serveur Splunk
- Création et modification arbitraire de fichiers
- Contournement des mécanismes d'authentification
- Atteinte à la confidentialité, à l'intégrité et à la disponibilité des données

SYSTÉME AFFECTÉ :

- Splunk Enterprise 10.0.x antérieures à 10.0.7
- Splunk Enterprise 10.2.x antérieures à 10.2.4

DÉSCRIPTION :

Une vulnérabilité critique a été identifiée dans Splunk Enterprise. Son exploitation permet à un attaquant non authentifié d'effectuer des opérations arbitraires sur les fichiers via le composant PostgreSQL Sidecar Service exposé sur le réseau. Cette faiblesse peut être utilisée pour créer ou modifier des fichiers malveillants puis être chaînée afin d'obtenir une exécution de code arbitraire à distance (RCE), conduisant à une compromission complète du serveur Splunk.

Des preuves de concept (PoC) publiques sont disponibles, augmentant significativement le risque d'exploitation.

SOLUTION :

Mettre à jour immédiatement vers :

- Splunk Enterprise 10.0.7 ou version ultérieure
- Splunk Enterprise 10.2.4 ou version ultérieure

CONTOURNEMENT PROVISOIRE :

En attendant l'application des correctifs, l'éditeur recommande de désactiver le service PostgreSQL Sidecar lorsque cela est possible.

DOCUMENTATION :

CVE-2026-20253

- https://www.cve.org/CVERecord?id=CVE-2026-20253

Splunk Vulnerability Disclosure

- https://advisory.splunk.com/advisories/SVD-2026-0603

Known Exploited Vulnerabilities Catalog

- Known Exploited Vulnerabilities Catalog | CISA