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

Autorité Nationale de Cybersécurité

Djibouti le, 14-06-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Splunk Enterprise
Réference	1484
Date de Publication	2026-06-14
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Compromission complète du système
- Contournement de l'authentification

SYSTÉME AFFECTÉ :

- Splunk Enterprise versions antérieures à 10.2.4
- Splunk Enterprise versions antérieures à 10.0.7
- Splunk Cloud Platform versions antérieures à 10.4.2604.3
- Splunk Cloud Platform versions antérieures à 10.2.2510.14

DÉSCRIPTION :

Une vulnérabilité critique a été identifiée dans Splunk Enterprise. Son exploitation pourrait permettre à un attaquant non authentifié d'effectuer des opérations arbitraires sur des fichiers puis d'obtenir une exécution de code à distance sur le serveur affecté.

Une exploitation réussie peut conduire à une compromission complète du système, avec des impacts potentiels sur la confidentialité, l'intégrité et la disponibilité des données.

SOLUTION :

Mettez à niveau Splunk Enterprise vers les versions 10.4.0, 10.2.4 et 10.0.7 ou supérieures.

DOCUMENTATION :

CVE-2026-20253 :

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

Splunk Vulnerability Disclosure :

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