AVIS DE SECURITE

Objet	**Vulnérabilité d'exécution de code à distance dans Cisco UCS Central Software**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-299
TLP	WHITE

Résumé

Cisco a publié le 04/11/2026 un avis de sécurité corrigeant la vulnérabilité CVE-2026-76506 (CVSS v3.1 : 7.6) affectant l'interface de gestion web de Cisco UCS Central Software. Due à une validation insuffisante des données fournies dans les requêtes HTTP (traversée de répertoires, CWE-22), elle permet à un attaquant distant authentifié, au moyen d'une requête HTTP forgée, d'exécuter des commandes arbitraires, d'écrire des fichiers arbitraires sur le système et d'accéder à des données sensibles. Aucun contournement n'est disponible. Cisco n'a connaissance d'aucune exploitation active à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données (écriture de fichiers arbitraires)

Systèmes affectés

- Cisco UCS Central Software versions 2.0 et antérieures (migrer vers une version corrigée)
- Cisco UCS Central Software versions 2.1 antérieures à 2.1(2c)
- Version corrigée : Cisco UCS Central Software 2.1(2c)

Recommandations

1. Mettre à jour Cisco UCS Central Software vers la version 2.1(2c), aucun contournement n'étant disponible, et restreindre l'accès à l'interface de gestion web aux seuls réseaux d'administration.
2. Se référer au bulletin de sécurité de l'éditeur du 04/11/2026 (cisco-sa-cucs-rce-LzHSFRDQ, bogue CSCwv60193) :
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucs-rce-LzHSFRDQ
   - https://nvd.nist.gov/vuln/detail/CVE-2026-76506
   - https://www.cve.org/CVERecord?id=CVE-2026-76506

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

E-mail : sncsirt@dcssi.sn

Date de publication : 05/11/2026