AVIS DE SECURITE

Objet	Vulnérabilité critique de contournement d'authentification dans Cisco Identity Services Engine (ISE)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-205
TLP	WHITE

Résumé

Cisco a publié le 16 septembre 2026 un correctif pour une vulnérabilité critique (CVE-2026-76460, CVSS 10.0) affectant une API de Cisco Identity Services Engine (ISE) et de Cisco ISE Passive Identity Connector (ISE-PIC). Un défaut de contrôle d'authentification sur un point de terminaison API permet à un attaquant distant non authentifié de contourner l'interface web d'administration et d'obtenir un accès non autorisé au dispositif. Cisco confirme une exploitation active et la CISA a ajouté cette vulnérabilité à son catalogue des vulnérabilités activement exploitées (KEV) le 16 septembre 2026, avec une échéance de correction fixée au 19 septembre 2026 pour les agences fédérales américaines.

Risque de sécurité

- Contournement de l'authentification et de la politique de sécurité
- Accès administrateur non autorisé au dispositif via l'interface web de gestion
- Atteinte à la confidentialité, à l'intégrité et à la disponibilité des données (CVSS 10.0)

Systèmes affectés

- Cisco Identity Services Engine (ISE) — versions antérieures aux correctifs publiés le 16 septembre 2026
- Cisco ISE Passive Identity Connector (ISE-PIC), quelle que soit la configuration du dispositif

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 16 septembre 2026 :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html