AVIS DE SECURITE

Objet	Vulnérabilité critique de contournement d'autorisation sur l'API REST de Cisco Identity Services Engine (ISE)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-215
TLP	WHITE

Résumé

Cisco a publié le 16 septembre 2026 l'avis de sécurité cisco-sa-ISE-ABP-VNSW7Tn5 révélant CVE-2026-76423, une vulnérabilité critique cotée CVSS 10.0 par Cisco PSIRT, confirmée par le NVD. Le service web de l'API REST de Cisco Identity Services Engine (ISE) et ISE Passive Identity Connector (ISE-PIC) est exposé avec des contrôles d'autorisation insuffisants, permettant à un attaquant distant non authentifié d'obtenir un accès administrateur complet et de lire ou modifier la configuration et les données d'identité d'ISE. Cette vulnérabilité est distincte de CVE-2026-76460 (contournement d'authentification sur l'interface de gestion web, déjà couverte par le bulletin SNCSIRT-2026-ADS-205 du 17/09/2026, activement exploitée et ajoutée au catalogue CISA KEV) ; aucune exploitation active n'est signalée à ce jour pour CVE-2026-76423.

Risque de sécurité

- Contournement de la politique de sécurité / élévation de privilèges via l'API REST (CVE-2026-76423, CVSS 10.0)
- Accès administrateur non autorisé à la plateforme ISE
- Atteinte à la confidentialité et à l'intégrité des données de configuration et d'identité
- Compromission potentielle de l'infrastructure d'authentification réseau dépendante d'ISE

Systèmes affectés

- Cisco ISE et ISE-PIC versions antérieures à 3.1 Patch 12
- Cisco ISE versions 3.2 antérieures à Patch 11
- Cisco ISE versions 3.3 antérieures à Patch 12
- Cisco ISE versions 3.4 antérieures à Patch 7
- Cisco ISE versions 3.5 antérieures à Patch 4
- Branche 3.0 : fin de support depuis le 13 juillet 2025, non corrigée — migration vers une version supportée requise

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 16 septembre 2026 :
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5 (bulletin de sécurité Cisco)
   - https://www.cve.org/CVERecord?id=CVE-2026-76423 (référence CVE)

2. Appliquer sans délai le correctif applicable : 3.1 Patch 12, 3.2 Patch 11, 3.3 Patch 12, 3.4 Patch 7 ou 3.5 Patch 4