AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques additionnelles dans Cisco Identity Services Engine (ISE), durcissement logiciel
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-206
TLP	WHITE

Résumé

Parallèlement au correctif d'urgence pour la vulnérabilité activement exploitée CVE-2026-76460 (cf. SNCSIRT-2026-ADS-203), l'équipe d'ingénierie de Cisco Identity Services Engine (ISE) et ISE Passive Identity Connector (ISE-PIC) a publié le 16 septembre 2026, à l'issue d'une revue de sécurité interne, une release de durcissement logiciel corrigeant plusieurs vulnérabilités découvertes en interne, dont deux atteignant le score CVSS maximal de 10.0. Cisco indique n'avoir connaissance d'aucune exploitation active de ces vulnérabilités, distinctes de CVE-2026-76460.

Risque de sécurité

- Contournement du contrôle d'accès (CVE-2026-20192, CVSS 10.0)
- Neutralisation incorrecte d'éléments spéciaux / injection (CVE-2026-20130, CVSS 10.0)
- Divulgation d'identifiants insuffisamment protégés (CVE-2026-20234, CVSS 9.9)
- Transfert incorrect de ressources entre sphères (CVE-2026-20194, CVSS 9.1)
- Validation d'entrée incorrecte (CVE-2026-20237, CVSS 9.1)

Systèmes affectés

- Cisco Identity Services Engine (ISE) — versions couvertes par le bulletin de durcissement du 16 septembre 2026
- Cisco ISE Passive Identity Connector (ISE-PIC)

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-hardening-ise-XU5EwX5T