AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques additionnelles dans Cisco Secure Email Gateway et Secure Email and Web Manager (durcissement logiciel)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-203
TLP	WHITE

Résumé

Le 14 septembre 2026, en complément de l'avis cisco-sa-esa-inj-2bLVGmhX portant sur la vulnérabilité d'injection SQL activement exploitée CVE-2026-76461 (couverte par le bulletin SNCSIRT-2026-ADS-202 du 15/09/2026), Cisco a publié un second avis, cisco-sa-hardening-esa-dfCrfXkm, à l'issue d'une revue de sécurité interne de ses produits Secure Email Gateway (AsyncOS) et Secure Email and Web Manager. Cet avis corrige quatre vulnérabilités critiques distinctes (CVE-2026-76440, CVE-2026-76441, CVE-2026-20353 et CVE-2026-76443), toutes notées CVSS 9.8, affectant les appliances physiques et virtuelles quelle que soit leur configuration. Cisco indique n'avoir constaté aucune exploitation active de ces quatre vulnérabilités à ce jour, mais recommande une mise à jour sans délai compte tenu de leur sévérité.

Risque de sécurité

- Traversée de chemin (path traversal) permettant l'accès à des fichiers restreints du système (CVE-2026-76440, CVSS 9.8)
- Contournement des contrôles d'accès permettant la réalisation d'actions non autorisées (CVE-2026-76441, CVSS 9.8)
- Consommation incontrôlée de ressources et erreurs de désérialisation lors du traitement des données (CVE-2026-20353, CVSS 9.8)
- Neutralisation incorrecte des entrées pouvant conduire à des injections de commandes ou SQL (CVE-2026-76443, CVSS 9.8)
- Compromission potentielle de la passerelle de messagerie et rebond possible vers l'infrastructure interne

Systèmes affectés

- Cisco Secure Email Gateway (AsyncOS), versions 16.0.x antérieures à 16.0.4-3021
- Cisco Secure Email Gateway (AsyncOS), versions 16.5.x antérieures à 16.5.0-780
- Cisco Secure Email Gateway (AsyncOS), versions antérieures à 15.5.5-0141
- Cisco Secure Email and Web Manager, versions 16.x antérieures à 16.5.0-429
- Cisco Secure Email and Web Manager, versions antérieures à 15.5.5-006
- Déploiements physiques et virtuels des appliances concernées, indépendamment de la configuration

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 14 septembre 2026 (cisco-sa-hardening-esa-dfCrfXkm) :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm