AVIS DE SECURITE

Objet	Vulnérabilité critique d'injection SQL non authentifiée dans Cisco Secure Email Gateway, activement exploitée (CISA KEV)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-202
TLP	WHITE

Résumé

Le 14 septembre 2026, Cisco a publié l'avis de sécurité cisco-sa-esa-inj-2bLVGmhX pour une vulnérabilité d'injection SQL non authentifiée (CVE-2026-76461, CVSS 9.8) dans la logique d'analyse des e-mails du logiciel AsyncOS de Cisco Secure Email Gateway (anciennement ESA) et Cisco Secure Email and Web Manager. Un attaquant distant non authentifié peut exploiter la faille en envoyant un e-mail spécialement conçu contenant des instructions SQL malveillantes, qui sont exécutées sans contrôle lors du traitement du message, permettant l'exécution de commandes arbitraires avec les privilèges root du système d'exploitation sous-jacent. Cisco PSIRT a confirmé une exploitation active de cette vulnérabilité en septembre 2026 ; elle a été ajoutée au catalogue CISA KEV le 14 septembre 2026, avec une échéance fédérale de correction fixée au 17 septembre 2026. Aucun contournement n'est disponible ; Cisco recommande une mise à jour immédiate vers une version corrigée d'AsyncOS.

Risque de sécurité

- Exécution de code arbitraire à distance avec privilèges root, sans authentification (CVE-2026-76461, CVSS 9.8, injection SQL — CWE-89)
- Atteinte à la confidentialité, à l'intégrité et à la disponibilité du système sous-jacent
- Compromission complète de la passerelle de messagerie et rebond possible vers l'infrastructure interne

Systèmes affectés

- Cisco Secure Email Gateway (AsyncOS), versions antérieures à 16.5.0-780, 16.0.4-3021 et 15.5.5-0141
- Cisco Secure Email and Web Manager, déploiements AsyncOS exposés à la même logique d'analyse des e-mails
- Déploiements physiques et virtuels des appliances concernées

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 14 septembre 2026 (cisco-sa-esa-inj-2bLVGmhX) :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX
- https://www.cisa.gov/news-events/alerts/2026/09/14/cisa-adds-one-known-exploited-vulnerability-catalog