AVIS DE SECURITE

Objet	**Vulnérabilité critique exploitée dans Cisco AsyncOS pour Secure Email Gateway (CVE-2026-76519)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-262
TLP	WHITE

Résumé

Cisco a publié le 14/10/2026 un correctif pour la vulnérabilité CVE-2026-76519 (CVSS v3.1 : 9.8) affectant la fonctionnalité Advanced Malware Protection de Cisco Secure Email Gateway. Lorsque la réputation des fichiers est activée, un attaquant non authentifié peut, via une pièce jointe spécialement conçue, écrire des fichiers arbitraires sur le système sous-jacent et exécuter des commandes avec les privilèges root. Cisco indique que cette vulnérabilité est activement exploitée.

Risque de sécurité

- Exécution de code arbitraire à distance
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Compromission complète du système (privilèges root)

Systèmes affectés

- Cisco AsyncOS Software pour Secure Email Gateway 15.5.x antérieures à 15.5.5-014
- Cisco AsyncOS Software pour Secure Email Gateway 16.x antérieures à 16.5.0-780
- Configuration vulnérable : fonctionnalité Advanced Malware Protection avec réputation des fichiers (File Reputation) activée

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 14/10/2026 :
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp
2. Mettre à jour Cisco AsyncOS pour Secure Email Gateway vers une version corrigée sans délai (exploitation active signalée)
3. Vérifier l'absence de compromission des équipements exposés avant et après la mise à jour