ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité zero-day critique activement exploitée dans Cisco AsyncOS Email Security Appliances
Numéro de Référence	59421812/25
Date de Publication	18 Décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco AsyncOS Email Security Appliances :
  - Cisco Secure Email Gateway (SEG)
  - Cisco Secure Email and Web Manager (SEWM)

Identificateurs externes

- CVE-2025-20393 ;

Bilan de la vulnérabilité

Cisco a identifié une campagne de cyberattaques active visant certains équipements Cisco Secure Email Gateway (SEG) et Cisco Secure Email and Web Manager (SMA) utilisant le système Cisco « AsyncOS ». Cisco a publié à ce titre un avis de sécurité critique concernant une vulnérabilité zero-day de sévérité maximale, référencée « CVE-2025-20393 », actuellement exploitée dans la nature. Cette faille permet à un attaquant distant sans authentification de prendre le contrôle total des équipements vulnérables en exécutant des commandes arbitraires avec les privilèges "root", exposant les systèmes affectés à un risque élevé de compromission, de persistance malveillante et de perte de contrôle.

L'exploitation de cette vulnérabilité n'est possible que si la fonctionnalité « Spam Quarantine » est activée sur l'équipement et si le port associé à « Spam Quarantine » est exposé et accessible depuis Internet. Lorsque ces deux conditions sont réunies, toutes les versions de Cisco AsyncOS sont considérées comme vulnérables.

Solution

En attendant la publication d'une mise à jour de sécurité, il est recommandé d'appliquer les mesures suivantes :

- Restreindre ou supprimer l'exposition à Internet des équipements concernés ;
- Limiter l'accès aux adresses IP de confiance et séparer les interfaces de gestion ;
- Désactiver l'accès aux services non nécessaires (HTTP, FTP, etc.) ;
- Surveiller les journaux afin de détecter toute activité suspecte ;
- Mettre en place une authentification forte et modifier les identifiants par défaut.

Veuillez se référer au bulletin de sécurité Cisco du 17 Décembre 2025 pour plus d'information.

Risque

- Elévation de privilège ;
- Accès aux informations confidentielles ;
- Exécution de commande arbitraire ;
- Persistance ;
- Prise de contrôle du système affecté ;

Indicateurs de compromission :

Hash :

- 2db8ad6e0f43e93cc557fbda0271a436f9f2a478b1607073d4ee3d20a87ae7ef
- 145424de9f7d5dd73b599328ada03aa6d6cdcee8d5fe0f7cb832297183dbe4ca
- 85a0b22bd17f7f87566bd335349ef89e24a5a19f899825b4d178ce6240f58bfc

IP :

- 172[.]233[.]67[.]176
- 172[.]237[.]29[.]147
- 38[.]54[.]56[.]95

Annexe

Bulletins de sécurité du Cisco du 17 Décembre 2025:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4