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	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	60061601/26
Date de Publication	16 Janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

Produits affectés par le zero-day « CVE-2025-20393 » :

- Cisco Secure Email Gateway :
  - Cisco AsyncOS 14.2 et versions antérieures
  - Cisco AsyncOS 15.0
  - Cisco AsyncOS 15.5
  - Cisco AsyncOS 16.0
- Cisco Secure Email and Web Manager :
  - Cisco AsyncOS 15.0 et versions antérieures
  - Cisco AsyncOS 15.5
  - Cisco AsyncOS 16.0
- N.B : Ces produits sont vulnérables lorsque :
  - la fonctionnalité Spam Quarantine est activée et exposée à Internet

Les vulnérabilités restantes affectent les produits suivants :

- Cisco ISE 3.2, 3.3, 3.4 ;
- Cisco EPNM 7.1, 8.0, 8.1 ;
- Cisco Prime Infrastructure 3.10;

Identificateurs externes

- CVE-2026-20076, CVE-2026-20047, CVE-2026-20075, CVE-2025-20393 ;

Bilan de la vulnérabilité

Cisco a publié des correctifs de sécurité pour plusieurs vulnérabilités critiques affectant les produits susmentionnées. Parmi celles-ci figure une vulnérabilité « zero-day », référencée « CVE-2025-20393 », résultant d'une validation insuffisante des requêtes HTTP dans

la fonctionnalité « Spam Quarantine ». Cette faille peut être exploitée par un attaquant distant non authentifié via l'envoie de requête spécialement conçue, lui permettant d'exécuter des commandes arbitraires avec les privilèges « root » sur les équipements vulnérables.

Par ailleurs, l'exploitation des autres vulnérabilités peut permettre à un attaquant authentifié d'exécuter du code JavaScript arbitraire dans le navigateur des utilisateurs ciblés ou d'accéder à des informations sensibles.

Solution

Cisco recommande l'application immédiate des mises à jour de sécurité du 15 Janvier 2026 afin de réduire les risques de compromission.

Risque

- Exécution du code arbitraire à distance ;
- Exécution de commandes arbitraires à distance ;
- Élévation de privilèges;
- Contournement des mécanismes et politiques de sécurité ;

Références

Bulletin de sécurité Cisco du 15 Janvier 2026:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-stored-xss-GEkX8yWK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-964cdxW5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-9TDh2kx

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma