ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Cisco
Numéro de Référence	60740502/26
Date de publication	05 février 2026
Risque	Important
Impact	Important

Systèmes affectés

- Cisco AsyncOS for Cisco Secure Web Appliance - versions antérieure à 15.2.5-011
- Cisco Evolved Programmable Network Manager (EPNM) – versions antérieure à 8.1.1
- Cisco Meeting Management Release – versions antérieure à 3.12.1 MR
- Cisco Prime Infrastructure – versions antérieure à 3.10.6 Security Update 2
- Cisco TelePresence CE Software in Cloud-Aware Operation – versions antérieure à RoomOS October 2025 Release
- Cisco TelePresence CE Software in Cloud-Aware Operation – versions antérieure à RoomOS December 2025 Release
- Cisco RoomOS Software in Cloud-Aware Operation – versions antérieure à RoomOS October 2025 Release
- Cisco RoomOS Software in Cloud-Aware Operation – versions antérieure à RoomOS December 2025 Release
- Cisco TelePresence CE Software in On-Premises Operation – versions antérieure à 11.27.5.0 and 11.32.3.0
- Cisco RoomOS Software in On-Premises Operation – versions antérieure à 11.27.5.0 and 11.32.3.0

Identificateurs externes

- CVE-2026-20119 CVE-2026-20098 CVE-2026-20056 CVE-2026-20111
- CVE-2026-20123

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'injecter du contenu dans une page, de contourner des mesures de sécurité, d'accéder à des informations confidentielles ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos produits.

Risques

- Injection de contenu dans une page
- Contournement de mesures de sécurité
- Accès à des informations confidentielles
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tce-roomos-dos-9V9jrC2q
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-file-up-kY47n8kK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-archive-bypass-Scx2e8zF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-xss-bYeVKCD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-redirect-6sX82dN

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma