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 dans les produits Cisco
Numéro de Référence	56530409/25
Date de Publication	04 Septembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Cisco Secure Firewall Threat Defense (FTD) pour Cisco Firepower 3100 et 4200 Series
- Cisco Unified CM et Unified CM SME version 12.5, 14 et 15
- Cisco Unified CM IM&P version 12.5, 14 et 15
- Cisco Evolved Programmable Network Manager (EPNM) version 8.0 et 8.1
- Cisco Prime Infrastructure version 3.9 et 3.10
- Cisco SIP 2.x, 3.x, 11.x et 14.x
- Cisco Desk Phone 9800 Series, IP Phone 7800 et 8800 Series, et Video Phone 8875
- Cisco Webex Meetings

Identificateurs externes

- CVE-2025-20270 CVE-2025-20280 CVE-2025-20287
- CVE-2025-20291 CVE-2025-20326 CVE-2025-20328
- CVE-2025-20327 CVE-2025-20330 CVE-2025-20335
- CVE-2025-20336

Bilan de la vulnérabilité

Cisco a publié des correctifs de sécurité pour les produits susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité des données et de réussir une injection de code indirecte à distance (XSS).

Solution

Veuillez se référer au bulletin de sécurité Cisco du 03 Septembre 2025 pour plus d'information.

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Exécution du code arbitraire à distance
- Injection de code indirecte à distance
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité Cisco du 03 Septembre 2025:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-csrf-w762pRYd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epni-arb-file-upload-jjdM2P83
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-info-dis-zhPPMfgz
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-stored-xss-XjQZsyCP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-xss-XQgu4HSG
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-write-g3kcC5Df
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-urlredirect-uK8dDJSZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-55bv8hhm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3100_4200_tlsdos-2yNSCd54