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	62442603/26
Date de publication	26 Mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Catalyst SD-WAN Manager
- Cisco IOS Software
- Cisco IOS XE Software
- Cisco IOS XE Wireless Controller Software
- Cisco Secure Firewall Adaptive Security Appliance Software
- Cisco Secure Firewall Threat Defense Software

Identificateurs externes

CVE-2026-20004 CVE-2026-20012 CVE-2026-20083 CVE-2026-20084 CVE-2026-20086
CVE-2026-20104 CVE-2026-20108 CVE-2026-20110 CVE-2026-20112 CVE-2026-20113
CVE-2026-20114 CVE-2026-20115 CVE-2026-20125 CVE-2026-20131

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'exécuter du code à distance, de contourner des mesures de sécurité, d'accéder à des informations confidentielles, d'élever ses privilèges ou de causer un déni de service.

Solution

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

Risques

- Exécution de code à distance
- Contournement de mesures de sécurité
- Accès à des informations confidentielles
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ios-dos-kPEpQGGK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootp-WuBhNBxA
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-dos-sbv8XRpL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-lobby-privesc-KwxBqJy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mntc-dos-LZweQcyq
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-tls-dos-TVgLDEZL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe_infodis-6J847uEB
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-crlf-NvgKTKJZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-xss-LpGkzwtJ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scp-dos-duAdXtCg
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-xss-ZqkhP9W9

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh