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	57062509/25
Date de publication	25 septembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Cisco IOS XE Software for Catalyst 9800 Series
- Cisco Wireless Access Point Software
- Cisco IOS XE Software on Cisco Catalyst 9500X and 9600X Series Switches
- Cisco SD-WAN vEdge Software
- Cisco IOS and IOS XE Software
- Cisco IOS XE Software for Catalyst 9000 Series Switches

Identificateurs externes

CVE-2025-20149 CVE-2025-20160 CVE-2025-20293 CVE-2025-20311 CVE-2025-20312
CVE-2025-20313 CVE-2025-20314 CVE-2025-20315 CVE-2025-20316 CVE-2025-20327
CVE-2025-20334 CVE-2025-20338 CVE-2025-20339 CVE-2025-20340 CVE-2025-20364
CVE-2025-20365

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 des commandes dans une page, de contourner des mesures de sécurité, d'accéder à des informations confidentielles ou de causer un déni de service

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

Solution

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

Risques

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

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-9800cl-openscep-SB4xtxzP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-action-frame-inj-QqCNcz8H
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat9k-acl-L4K7VXgD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-defaultacl-pSJk9nVF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-cli-EB7cZ6yO
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-arg-inject-EyDDbh4e
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-xss-VWyDgjOU
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat9k-PtmD7bgy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-invalid-url-dos-Nvxszf6u
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nbar-dos-LAvwTmeT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secboot-UqFD8AvC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmpwred-x3MJyf5M

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