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 plusieurs produits de Cisco
Numéro de Référence	46782803/24
Date de publication	28 Mars 2024
Risque	Important
Impact	Important

Systèmes affectés

- Cisco IOS XE Software
- Cisco Access Point Software
- Cisco IOS
- Cisco IOS Software for Catalyst 6000 Series Switches
- Cisco IOS XE Software for Wireless LAN Controllers
- Cisco Access Point Software
- Cisco Aironet Access Point
- Cisco Catalyst Center

Identificateurs externes

CVE-2024-20259	CVE-2024-20265	CVE-2024-20271	CVE-2024-20276
CVE-2024-20278	CVE-2024-20303	CVE-2024-20306	CVE-2024-20307
CVE-2024-20308	CVE-2024-20309	CVE-2024-20311	CVE-2024-20312
CVE-2024-20313	CVE-2024-20314	CVE-2024-20316	CVE-2024-20324
CVE-2024-20333	CVE-2024-20354		

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'élever ses privilèges, de contourner les mesures de sécurité ou de causer un déni de service.

Solution

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

Risques

- Déni de service
- Contournement de mesures de sécurité
- Accès à des informations confidentielles

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-airo-ap-dos-PPPtcVW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-h9TGGX6W
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-secureboot-bypass-zT5vJkSD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aux-333WBz8f
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccc-authz-bypass-5EKchJRb
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dhcp-dos-T3CXPO9z
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dmi-acl-bypass-Xv8FO8Vz
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-priv-esc-seAx6NLX

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-utd-cmd-JbL8KvHT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-wlc-privesc-RjSMrmPK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-sGjyOUHX
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lisp-3gYXs3qP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-mdns-dos-4hv6pBGf

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