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	40952303/23
Date de publication	23 Mars 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco IOS XE Software
- Cisco DNA Center
- Cisco IOS XE SD-WAN Software
- Cisco IOS XE Software for Wireless Association
- Cisco Access Point Software
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches
- Cisco IOS XE Software for Wireless LAN Controllers
- Cisco SD-WAN vManage Software
- Cisco Adaptive Security Appliance Software, Firepower Threat Defense Software, IOS Software, and IOS XE Software
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software
- Cisco Access Point Software

Identificateurs externes

CVE-2023-20072	CVE-2023-20027	CVE-2023-20080	CVE-2023-20065
CVE-2023-20055	CVE-2023-20035	CVE-2023-20067	CVE-2023-20112
CVE-2023-20082	CVE-2023-20066	CVE-2023-20056	CVE-2023-20100
CVE-2023-20113	CVE-2023-20081	CVE-2023-20107	CVE-2023-20097
CVE-2023-20059	CVE-2023-20029		

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 distant d'injecter des commandes, d'élever ses privilèges, de contourner des mesures de sécurité, d'accéder à des données confidentielles ou de causer un déni de service.

Solution

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

Risques

- Injection de commandes
- Elévation de privilège
- Contournement de mesures de sécurité
- Accès à des données confidentielles
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv4-vfr-dos-CXxtFacb
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw

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

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-dos-wFujBHKw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-assoc-dos-D2SunWK2
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-apjoin-dos-nXRHkt5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-csrf-76RDbLEh
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa5500x-entropy-6v9bHVYP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironetap-cmdinj-6bjT4FL8
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-pe7zAbdR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-priv-esc-sABD8hcU

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