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 plusieurs produits Cisco
Numéro de Référence	49732609/24
Date de Publication	26 Septembre 2024
Risque	Important
Impact	Important

Systèmes affectés

- Cisco IOS XE Software Web UI
- Cisco Catalyst 9000 Series Switches
- Cisco Catalyst Center Static SSH Host Key Vulnerability
- Cisco Catalyst SD-WAN Manager
- Cisco Catalyst SD-WAN Routers
- Cisco IOS Software on Cisco Industrial Ethernet Series Switches
- Cisco IOS XE Software HTTP Server Telephony Services
- Cisco IOS XE Software IPv4 Fragmentation Reassembly
- Cisco IOS XE Software Protocol Independent Multicast
- Cisco IOS XE Software SD-Access Fabric Edge Node
- Cisco IOS and IOS XE Software Resource Reservation Protocol
- Cisco IOS and IOS XE Software Web UI
- Cisco SD-WAN vEdge Software UDP Packet Validation
- Cisco Unified Threat Defense Snort Intrusion Prevention System Engine pour Cisco IOS XE

Identificateurs externes

- CVE-2024-20350 CVE-2024-20381 CVE-2024-20414 CVE-2024-20433 CVE-2024-20434 CVE-2024-20436 CVE-2024-20437 CVE-2024-20455 CVE-2024-20464 CVE-2024-20465 CVE-2024-20467 CVE-2024-20475 CVE-2024-20480 CVE-2024-20496 CVE-2024-20508

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités dans les produits Cisco susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant de causer un déni de service, de réussir une élévation de privilèges, d'exécuter du code arbitraire et de divulguer des informations confidentielles.

Solution

Veuillez se référer au bulletin de sécurité Cisco afin d'installer les nouvelles mises à jour.

Risque

- Elévation de privilèges
- Déni de service
- Exécution du code arbitraire à distance
- Divulgation des informations confidentielles

Annexe

Bulletins de sécurité Cisco du 25 Septembre 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-httpsrvr-dos-yOZThut
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ssh-e4uOdASj
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpp-vfr-dos-nhHKGgO
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vlan-dos-27Pur5RT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-utd-snort3-dos-bypas-b4OUEwxD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-xss-zQ4KPvYd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-repacl-9eXgnBpD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-HfwnRgk
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-cwa-acl-nPSbHSnA

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: 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-webui-csrf-ycUYxkKO
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rsvp-dos-OypvgVZf
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pim-APbVfySJ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-MBcbG9k