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	Vulnérabilité critique dans les produits Cisco
Numéro de Référence	51340512/24
Date de Publication	05 Décembre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches (both ACI et stetalone modes)
- UCS 6400 et 6500 Series Fabric Interconnects

Identificateurs externes

- CVE-2024-20397

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans le bootloader du logiciel Cisco NX-OS. Un attaquant pourrait exploiter cette vulnérabilité en exécutant une série de commandes afin de contourner la vérification de la signature de l'image NX-OS et de charger des logiciels non vérifiés.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 04 décembre 2024, afin d'installer les dernières mises à jour.

Risque

- Contournement de la politique de sécurité

Références

Bulletin de sécurité Cisco du 04 décembre 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma