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 critiques dans les produits Cisco
Numéro de Référence	50301810/24
Date de Publication	18 Octobre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco Unified CCMP versions 12.6.x antérieures à 12.6(1)_ES13
- Cisco UCS Central versions 2.0 antérieures à 2.0(1v)
- ATA 191 Analog Telephone Adapter versions 12.0.x antérieures 12.0.2
- ATA 191 and 192 Multiplatform Analog Telephone versions antérieures à 11.2.5

Identificateurs externes

- CVE-2024-20420 CVE-2024-20421 CVE-2024-20458 CVE-2024-20459
- CVE-2024-20460 CVE-2024-20461 CVE-2024-20462 CVE-2024-20463
- CVE-2024-20512 CVE-2024-20280

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Cisco susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de réussir une élévation de privilèges, de contourner la politique de sécurité, d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 16 Octobre 2024, afin d'installer les dernières mises à jour.

Risque

- Elévation de privilèges
- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité

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

- Déni de service à distance
- Atteinte à la confidentialité des données

Références

Bulletin de sécurité Cisco du 16 Octobre 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsc-bkpsky-TgJ5f73J
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmpdm-rxss-tAX76U3k