AVIS DE SECURITE

Objet	Vulnérabilités critiques dans les produits Cisco
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2024-ADS-228
TLP	WHITE

Résumé

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Cisco.

Risque de sécurité

- Elévation de privilèges
- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité
- Déni de service à distance
- Atteinte à la confidentialité des données

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

Recommandations

Se référer au Bulletin de sécurité de 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