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 les produits Cisco
Numéro de Référence	43801509/23
Date de Publication	15 Septembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- ConfD versions 7.4.x antérieures à 7.4.3.1
- ConfD versions 7.5.x antérieures à 7.5.2.1
- ConfD versions 7.6.x antérieures à 7.6.14.1
- ConfD versions 7.7.x antérieures à 7.7.13
- ConfD versions 7.8.x antérieures à 7.8.11
- ConfD versions 8.0.x antérieures à 8.0.8
- ConfD versions 8.1.x antérieures à 8.1.4
- Emergency Responder version 12.5(1)SU4 antérieure à 12.5(1)SU5 sans le correctif de sécurité ciscocm.CSCwh34565_PRIVILEGED_ACCESS_DISABLE.k4.cop.sha512
- Network Services Orchestrator versions 5.4.x antérieures à 5.4.3.2
- Network Services Orchestrator versions 5.5.x antérieures à 5.5.2.3
- Network Services Orchestrator versions 5.6.x antérieures à 5.6.14.1
- Network Services Orchestrator versions 5.7.x antérieures à 5.7.13
- Network Services Orchestrator versions 5.8.x antérieures à 5.8.11
- Network Services Orchestrator versions 6.0.x antérieures à 6.0.8
- Network Services Orchestrator versions 6.1.x antérieures à 6.1.3.1
- Unified CM IM&P version 12.5(1)SU7 antérieure à 12.5(1)SU8
- Unified CM IM&P version 14SU3 sans le correcif de sécurité ciscocm.cup_CSCwf62094_14SU3.cop.sha512
- Unified CM and Unified CM SME version 12.5(1)SU7 antérieure à 12.5(1)SU8

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

- Unified CM and Unified CM SME version 14SU3 sans le correctif de sécurité ciscocm.V14SU3_CSCwf44755.cop.sha512
- Unity Connection version 14SU3 sans le correcif de sécurité ciscocm.cuc.V14SU3_CSCwf62081.k4.cop.sha512

Identificateurs externes

- CVE-2021-1572, CVE-2023-20101, CVE-2023-20259

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, de réussir une élévation de privilège ou de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 04 Octobre 2023 pour plus d'information.

Risque

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

Annexe

Bulletins de sécurité Cisco du 04 Octobre 2023:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-apidos-PGsDcdNF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cer-priv-esc-B9t3hqk9