DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 19-10-2023

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Cisco
Réference	1056
Date de Publication	2023-10-05
Sévérité	Critique

IMPACT :

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

SYSTÉME AFFECTÉ :

- 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
- 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

DÉSCRIPTION :

Cisco a corrigé plusieurs vulnérabilités dans ses produits. Ces failles auraient pu être exploitées par un attaquant pour exécuter du code arbitraire à distance, obtenir un accès privilégié ou contourner les mesures de sécurité.

SOLUTION :

Vous trouverez des informations supplémentaires dans le bulletin de sécurité Cisco du 04 Octobre 2023.

DOCUMENTATION :

- 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

- CVE-2021-1572 :

https://www.cve.org/CVERecord?id=CVE-2021-1572

- CVE-2023-20101 :

https://www.cve.org/CVERecord?id=CVE-2023-20101

- CVE-2023-20259 :

https://www.cve.org/CVERecord?id=CVE-2023-20259