ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Cisco
Numéro de Référence	54920506/25
Date de publication	05 Juin 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco Identity Services Engine on Cloud Platforms
- Cisco Integrated Management Controller
- Cisco Nexus Dashboard Fabric Controller
- Cisco Unified Communications Products
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Identity Services Engine
- Cisco Unified Contact Center Express
- Cisco ThousandEyes Endpoint Agent for Windows
- Cisco Customer Collaboration Platform

Identificateurs externes

CVE-2025-20286	CVE-2025-20261	CVE-2025-20163	CVE-2025-20278
CVE-2025-20273	CVE-2025-20130	CVE-2025-20276	CVE-2025-20277
CVE-2025-20279	CVE-2025-20275	CVE-2025-20259	CVE-2025-20129

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'injecter des commandes, d'élever ses privilèges, d'accéder à des données confidentielles.

Solution

Veuillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos produits.

Risques

- Exécution de code arbitraire
- Injection de commandes
- Elévation de privilèges
- Accès à des données confidentielles

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccp-info-disc-ZyGerQpd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-icm-xss-cfcqhXAg
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-upload-P4M8vwXY
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-shkv-snQJtjrp
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-endagent-filewrt-zNcDqNRJ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-editor-rce-ezyYZte8
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-multi-UhOTvPGL
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vos-command-inject-65s2UCYy

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma