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 plusieurs produits de Cisco
Numéro de Référence	46870404/24
Date de publication	04 Avril 2024
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Nexus Dashboard Fabric Controller
- Cisco Nexus Dashboard and Nexus Dashboard
- Cisco Identity Services Engine
- Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers
- Cisco TelePresence Management Suite
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Enterprise Chat and Email
- Cisco Emergency Responder
- Cisco Nexus Dashboard Orchestrator
- Cisco Nexus Dashboard

Identificateurs externes

CVE-2024-20281 CVE-2024-20282 CVE-2024-20283 CVE-2024-20302
CVE-2024-20310 CVE-2024-20332 CVE-2024-20334 CVE-2024-20347
CVE-2024-20352 CVE-2024-20348 CVE-2024-20362 CVE-2024-20367
CVE-2024-20368

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 d'accéder à des informations confidentielles ou d'injecter du contenu dans une page.

Solution

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

Risques

- Accès à des informations confidentielles
- Injection de contenu dans une page

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cem-csrf-suCmNjFr
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imps-xss-quWkd9yF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-xss-CSQxgxfM
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-NfAKXrp5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-ssrf-FtSTh5Oz
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-dir-trav-SSn3AYDw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfccsrf-TEmZEfJ9
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-upav-YRqsCcSP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndru-pesc-kZ2PQLZH

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbiz-rv-xss-OQeRTup
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-kGw4DX9Y