**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** | 56442808/25 |
| **Date de publication** | 28 Aout 2025 |
| **Risque** | Important |
| **Impact** | Important |

**Systèmes affectés**

- Cisco Integrated Management
- Cisco Nexus 3000 and 9000 Series Switches
- Cisco Nexus Dashboard
- Cisco UCS Manager Software
- Cisco NX-OS Software
- Cisco Nexus Dashboard and Nexus Dashboard Fabric
- Cisco Integrated Management Controller

**Identificateurs externes**

CVE-2025-20241 CVE-2025-20262 CVE-2025-20290 CVE-2025-20292 CVE-2025-20294
CVE-2025-20295 CVE-2025-20296 CVE-2025-20317 CVE-2025-20342 CVE-2025-20344
CVE-2025-20347 CVE-2025-20348

## 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 de télécharger des fichiers malicieux, d'injecter des commandes, d'accéder à des informations confidentielles ou de causer un déni de service

**Solution**

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

**Risques**

- Téléchargement de fichiers malicieux
- Accès à des informations confidentielles
- Injection de commandes
- Déni de service

**Références**

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-vkvmorv-CnKrV7HK
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n39k-isis-dos-JhJA8Rfx
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-ptrs-XU2Fm2Wb
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-multi-cmdinj-E4Ukjyrz
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-infodis-TEcTYSFG
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nshs-urapi-gJuBVFpu
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-kvmsxss-6h7AnUyk
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-xss-Ey6XhyPS
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxospc-pim6-vG4jFPh
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmdinj-qhNze5Ss

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