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	57591610/25
Date de publication	16 octobre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Cisco TelePresence Collaboration Endpoint and RoomOS Software
- Cisco IOS XE Software
- Cisco Desk Phone 9800 Series, IP Phone 7800 and 8800 Series, and Video Phone 8875 with SIP Software
- Les produits suivants s'ils fonctionnent avec une version vulnérable de Unified Threat Defense (UTD) Snort IPS Engine for Cisco IOS XE Software ou UTD Engine for Cisco IOS XE SD-WAN Software:
  - ✓ 1000 Series Integrated Services Routers (ISRs)
  - ✓ 4000 Series ISRs
  - ✓ Catalyst 8000V Edge Software
  - ✓ Catalyst 8200 Series Edge Platforms
  - ✓ Catalyst 8300 Series Edge Platforms
  - ✓ Catalyst 8500L Edge Platforms
  - ✓ Cloud Services Routers 1000V

Identificateurs externes

- CVE-2025-20329 CVE-2025-20359 CVE-2025-20360 CVE-2025-20313
- CVE-2025-20314 CVE-2025-20350 CVE-2025-20351

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'injecter du contenu dans une page, d'exécuter du code, 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

- Injection de contenu dans une page
- Exécution de code
- Accès à des informations confidentielles
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-inf-disc-qGgsbxAm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-mime-vulns-tTL8PgVH
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secboot-UqFD8AvC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-dos-FPyjLV7A

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