**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** | Vulnérabilité critique activement exploitée affectant Cisco Unified Communications |
| **Numéro de Référence** | 60242201/26 |
| **Date de publication** | 22 janvier 2026 |
| **Risque** | Critique |
| **Impact** | Critique |

## Systèmes affectés

- Cisco Unified CM Unified CM SME 12.5, 14 et 15
- Cisco Unified CM IM&P 12.5, 14 et 15
- Cisco Unity Connection versions 12.5, 14 et 15
- Cisco Webex Calling Dedicated Instance 12.5, 14 et 15
- Cisco Packaged Contact Center Enterprise (Packaged CCE) versions 15.0, 12.6 et versions antérieures à 12.6
- Cisco Unified Contact Center Enterprise (Unified CCE) versions 15.0, 12.6 et versions antérieures à 12.6
- Cisco Intersight Virtual Appliance versions 1.1.4, 1.1.3 et versions antérieures à 1.1.3
- Cisco IEC6400 Wireless Backhaul Edge Compute Software versions 1.1.0 et antérieures

## Identificateurs externes

- CVE-2026-20045 CVE-2026-20055 CVE-2026-20109 CVE-2026-20092
- CVE-2026-20080

## Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. Une de ces vulnérabilité identifiée par « CVE-2026-20045 » et qui affecte certains produits de la suite Cisco Unified Communications est un « Zero-Day » activement exploité. Ces vulnérabilités peuvent permettre à un attaquant d'exécuter du code à distance, d'élever ses privilèges d'injecter du contenu dans un site ou de causer un déni de service.

## Solution

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

## Risques

- Exécution de code à distance
- Elévation de privilèges
- Injection de contenu dans un site (XSS)
- Déni de service

## Références

Bulletin de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iec6400-Pem5uQ7v
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-intersight-privesc-p6tBm6jk
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-xss-2JVyg3uD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b

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