ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	52092301/25
Date de Publication	23 Janvier 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco Meeting Management version 3.9.x et 3.8.x antérieure à 3.9.1
- Cisco BroadWorks version antérieure à RI.2024.11
- Secure Endpoint Connector pour Linux
- Secure Endpoint Connector pour Mac
- Secure Endpoint Connector pour Windows
- Secure Endpoint Private Cloud

Identificateurs externes

- CVE-2025-20156, CVE-2025-20165, CVE-2025-20128

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les versions susmentionnées des produits Cisco. L'exploitation de ces failles pourrait permettre à un attaquant distant et authentifié disposant de faibles privilèges d'élever ses privilèges à un utilisateur « root » ou de causer un déni de service sur un appareil affecté.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 22 Janvier 2025 pour plus d'information.

Risque

- Déni de service
- Elévation de privilèges

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Annexe

Bulletin de sécurité Cisco du 22 Janvier 2025:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-sip-dos-mSySbrmt
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-ole2-H549rphA