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 dans les produits Zoom
Numéro de Référence	54491405/25
Date de Publication	14 Mai 2025
Risque	Important
Impact	Important

Systèmes affectés

- Zoom Workplace Desktop App pour Windows version antérieure à 6.4.0
- Zoom Workplace Desktop App pour macOS version antérieure à 6.4.0
- Zoom Workplace Desktop App pour Linux version antérieure à 6.4.0
- Zoom Workplace App pour iOS version antérieure à 6.4.0
- Zoom Workplace VDI Client pour Windows version antérieure à 6.3.10 (sauf versions 6.1.17 et 6.2.13)
- Zoom Rooms Controller pour Windows version antérieure à 6.4.0
- Zoom Rooms Controller pour macOS version antérieure à 6.4.0
- Zoom Rooms Controller pour Linux version antérieure à 6.4.0
- Zoom Rooms Controller pour Android version antérieure à 6.4.0
- Zoom Rooms Client pour Windows version antérieure à 6.4.0
- Zoom Rooms Client pour macOS version antérieure à 6.4.0
- Zoom Rooms Client pour Android version antérieure à 6.4.0
- Zoom Rooms Client pour iPad version antérieure à 6.4.0
- Zoom Meeting SDK pour Windows version antérieure à 6.4.0
- Zoom Meeting SDK pour Android version antérieure à 6.4.0
- Zoom Meeting SDK pour macOS version antérieure à 6.4.0
- Zoom Meeting SDK pour Linux version antérieure à 6.4.0
- Zoom Workplace App pour Android version antérieure à 6.4.0
- Zoom Meeting SDK pour iOS version antérieure à 6.4.0

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

- Zoom Workplace VDI Client pour Windows version antérieure à 6.3.10
- Zoom Workplace VDI Client pour Windows version antérieure à 6.3.10 (sauf versions 6.1.16 et 6.2.12)

Identificateurs externes

- CVE-2025-30663, CVE-2025-30668, CVE-2025-46786, CVE-2025-46787,
- CVE-2025-46785, CVE-2025-30667, CVE-2025-30665, CVE-2025-30666,
- CVE-2025-30664

Bilan de la vulnérabilité

Zoom a publié des mises à jour de sécurité qui corrigent plusieurs vulnérabilités dans Zoom Workplace Apps et les produits associés. Ces vulnérabilités pourraient permettre à des attaquants d'élever leurs privilèges, de provoquer un déni de service, de lire des données confidentielles ou de contourner les contrôles de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Zoom du 13 Mai 2025 pour plus d'information.

Risque

- Elévation de privilèges
- Déni de service
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Zoom du 13 Mai 2025:

- https://www.zoom.com/en/trust/security-bulletin/?cms_guid=false&lang=null