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 Microsoft Office (Patch Tuesday Mars 2026)
Numéro de Référence	61841103/26
Date de Publication	11 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Office LTSC pour Mac 2024
- Microsoft Office LTSC 2024 pour 64-bit editions
- Microsoft Office LTSC 2024 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 64-bit editions
- Microsoft 365 Apps pour Enterprise pour 32-bit Systems
- Microsoft 365 Apps pour Enterprise pour 64-bit Systems
- Microsoft Office pour Android
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office LTSC pour Mac 2021
- Microsoft Office 2019 pour 64-bit editions
- Microsoft Office 2019 pour 32-bit editions
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2016 (32-bit edition)
- Office Online Server
- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016

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

Identificateurs externes

- CVE-2026-26107 CVE-2026-26144 CVE-2026-26110 CVE-2026-26109 CVE-2026-26108
- CVE-2026-26106 CVE-2026-26134 CVE-2026-26114 CVE-2026-26113 CVE-2026-26112
- CVE-2026-26105 CVE-2026-25180 CVE-2026-24285

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft office. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant de réussir une élévation de privilèges, de divulguer des informations confidentielles et d'exécuter du code arbitraire à distance.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 10 Mars 2026**.**

Risque

- Exécution du code arbitraire à distance ;
- Elévation de privilèges ;
- Divulgation des informations confidentielles ;

Annexe

Bulletin de sécurité Microsoft du 10 Mars 2026**:**

- https://msrc.microsoft.com/update-guide/

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