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 Microsoft Windows (Patch Tuesday Février 2026)
Numéro de Référence	60931102/26
Date de Publication	10 Février 2026
Risque	Important
Impact	Important

Systèmes affectés

- Windows App pour Mac 11.3.2
- Windows 10 Version 1607 pour x64-based Systems 10.0.14393.8868
- Windows 10 Version 1607 pour 32-bit Systems 10.0.14393.8868
- Windows Server 2025 10.0.26100.32370
- Windows Server 2025 10.0.26100.32313
- Windows 11 Version 24H2 pour x64-based Systems 10.0.26100.7840
- Windows 11 Version 24H2 pour x64-based Systems 10.0.26100.7781
- Windows 11 Version 24H2 pour ARM64-based Systems 10.0.26100.7840
- Windows 11 Version 24H2 pour ARM64-based Systems 10.0.26100.7781
- Windows Server 2022, 23H2 Edition (Server Core installation) 10.0.25398.2149
- Windows 11 Version 23H2 pour x64-based Systems 10.0.22631.6649
- Windows 11 Version 23H2 pour ARM64-based Systems 10.0.22631.6649
- Windows 11 Version 25H2 pour x64-based Systems 10.0.26200.7840
- Windows 11 Version 25H2 pour x64-based Systems 10.0.26200.7781
- Windows 11 Version 25H2 pour ARM64-based Systems 10.0.26200.7840
- Windows 11 Version 25H2 pour ARM64-based Systems 10.0.26200.7781
- Windows Server 2025 (Server Core installation) 10.0.26100.32370
- Windows Server 2025 (Server Core installation) 10.0.26100.32313
- Windows 10 Version 21H2 pour x64-based Systems 10.0.19044.6937
- Windows 10 Version 21H2 pour ARM64-based Systems 10.0.19044.6937

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

- Windows 10 Version 21H2 pour 32-bit Systems 10.0.19044.6937
- Windows Server 2022 (Server Core installation) 10.0.20348.4773
- Windows Server 2022 (Server Core installation) 10.0.20348.4711
- Windows Server 2022 10.0.20348.4773
- Windows Server 2022 10.0.20348.4711
- Windows Server 2019 (Server Core installation) 10.0.17763.8389
- Windows Server 2019 10.0.17763.8389
- Windows 10 Version 1809 pour x64-based Systems 10.0.17763.8389
- Windows 10 Version 1809 pour 32-bit Systems 10.0.17763.8389
- Windows Server 2016 (Server Core installation) 10.0.14393.8868
- Windows Server 2016 10.0.14393.8868
- Windows 11 version 26H1 pour x64-based Systems 10.0.28000.1575
- Windows 11 Version 26H1 pour ARM64-based Systems 10.0.28000.1575
- Windows 10 Version 22H2 pour 32-bit Systems 10.0.19045.6937
- Windows 10 Version 22H2 pour ARM64-based Systems 10.0.19045.6937
- Windows 10 Version 22H2 pour x64-based Systems 10.0.19045.6937
- Windows Server 2012 R2 (Server Core installation) 6.3.9600.23022
- Windows Server 2012 R2 6.3.9600.23022
- Windows Server 2012 (Server Core installation) 6.2.9200.25923
- Windows Server 2012 6.2.9200.25923

Identificateurs externes

- CVE-2026-20846 CVE-2026-21237 CVE-2026-21238 CVE-2026-21253
- CVE-2026-21513 CVE-2026-21234 CVE-2026-21247 CVE-2026-21222
- CVE-2026-21231 CVE-2026-21239 CVE-2026-21240 CVE-2026-21244
- CVE-2026-21249 CVE-2026-21255 CVE-2026-21508 CVE-2026-21525
- CVE-2026-21510 CVE-2026-21527 CVE-2026-21533 CVE-2026-21236
- CVE-2026-21235 CVE-2026-21242 CVE-2026-21246 CVE-2026-21248
- CVE-2026-21519 CVE-2026-21243 CVE-2026-21244 CVE-2026-21253
- CVE-2026-21525 CVE-2026-21513 CVE-2026-21234 CVE-2026-21247
- CVE-2026-21248 CVE-2026-21222 CVE-2026-21231 CVE-2026-21232
- CVE-2026-21238 CVE-2026-21239 CVE-2026-21241 CVE-2026-21245
- CVE-2026-21249 CVE-2026-21250 CVE-2026-21251 CVE-2026-21255

- CVE-2026-21508 CVE-2026-21510 CVE-2026-21533 CVE-2026-21236
- CVE-2026-21235 CVE-2026-21242 CVE-2026-21246 CVE-2026-21519

Bilan de la vulnérabilité

Microsoft a annoncé la correction de plusieurs vulnérabilités affectant les produits Microsoft Windows susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant d'élever ses privilèges, d'exécuter du code arbitraire à distance, de contourner des mécanismes de sécurité, de provoquer un déni de service, de divulguer des informations sensibles ou encore de réussir une usurpation d'identité.

Solution

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

Risque

- Élévation des privilèges ;
- Déni de service ;
- Divulgation d'informations confidentielles ;
- Exécution de code arbitraire à distance ;
- Contournement de la politique de sécurité ;
- Usurpation d'identité ;

Annexe

Bulletin de sécurité Microsoft du 10 Février 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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma