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 Avril 2026)
Numéro de Référence	63131504/26
Date de Publication	15 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 11 Version 23H2 pour x64-based Systems
- Windows 11 Version 23H2 pour ARM64-based Systems
- Windows 11 Version 25H2 pour x64-based Systems
- Windows 11 Version 25H2 pour ARM systems
- Windows Server 2025 (Server Core installation)
- Windows 10 Version 21H2 pour x64-based Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 11 version 26H1 pour x64-based Systems
- Windows 11 Version 26H1 pour ARM64-based Systems
- Windows Server 2025
- Windows Server 2022, 23H2 Edition (Server Core installation)

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 11 Version 24H2 pour x64-based Systems
- Windows 11 Version 24H2 pour ARM64-based Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Admin Center
- Remote Desktop client pour Windows Desktop
- Windows App Client pour Windows Desktop
- Windows Server 2012 R2 (Server Core installation)
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 22H2 pour x64-based Systems
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)

Identificateurs externes

- CVE-2026-0390 CVE-2026-20806 CVE-2026-20928 CVE-2026-20930 CVE-2026-23670
- CVE-2026-25184 CVE-2026-25250 CVE-2026-26151 CVE-2026-26152 CVE-2026-26153
- CVE-2026-26154 CVE-2026-26155 CVE-2026-26156 CVE-2026-26159 CVE-2026-26160
- CVE-2026-26161 CVE-2026-26162 CVE-2026-26163 CVE-2026-26165 CVE-2026-26166
- CVE-2026-26167 CVE-2026-26168 CVE-2026-26169 CVE-2026-26170 CVE-2026-26172
- CVE-2026-26173 CVE-2026-26174 CVE-2026-26175 CVE-2026-26176 CVE-2026-26177
- CVE-2026-26178 CVE-2026-26179 CVE-2026-26180 CVE-2026-26181 CVE-2026-26182
- CVE-2026-26183 CVE-2026-26184 CVE-2026-27906 CVE-2026-27907 CVE-2026-27908
- CVE-2026-27909 CVE-2026-27910 CVE-2026-27911 CVE-2026-27912 CVE-2026-27913
- CVE-2026-27914 CVE-2026-27915 CVE-2026-27916 CVE-2026-27917 CVE-2026-27918
- CVE-2026-27919 CVE-2026-27920 CVE-2026-27921 CVE-2026-27922 CVE-2026-27923
- CVE-2026-27924 CVE-2026-27925 CVE-2026-27926 CVE-2026-27927 CVE-2026-27928
- CVE-2026-27929 CVE-2026-27930 CVE-2026-27931 CVE-2026-32068 CVE-2026-32069
- CVE-2026-32070 CVE-2026-32071 CVE-2026-32072 CVE-2026-32073 CVE-2026-32074
- CVE-2026-32075 CVE-2026-32076 CVE-2026-32077 CVE-2026-32078 CVE-2026-32079
- CVE-2026-32080 CVE-2026-32081 CVE-2026-32082 CVE-2026-32083 CVE-2026-32084
- CVE-2026-32085 CVE-2026-32086 CVE-2026-32087 CVE-2026-32088 CVE-2026-32089

- CVE-2026-32090 CVE-2026-32091 CVE-2026-32093 CVE-2026-32149 CVE-2026-32150
- CVE-2026-32151 CVE-2026-32152 CVE-2026-32153 CVE-2026-32154 CVE-2026-32155
- CVE-2026-32156 CVE-2026-32157 CVE-2026-32158 CVE-2026-32159 CVE-2026-32160
- CVE-2026-32162 CVE-2026-32163 CVE-2026-32164 CVE-2026-32165 CVE-2026-32181
- CVE-2026-32183 CVE-2026-32195 CVE-2026-32196 CVE-2026-32202 CVE-2026-32212
- CVE-2026-32214 CVE-2026-32215 CVE-2026-32216 CVE-2026-32217 CVE-2026-32218
- CVE-2026-32219 CVE-2026-32220 CVE-2026-32221 CVE-2026-32222 CVE-2026-32223
- CVE-2026-32224 CVE-2026-32225 CVE-2026-33096 CVE-2026-33098 CVE-2026-33099
- CVE-2026-33100 CVE-2026-33101 CVE-2026-33104 CVE-2026-33824 CVE-2026-33826
- CVE-2026-33827 CVE-2026-33829

Bilan de la vulnérabilité

Microsoft a annoncé la correction de plusieurs vulnérabilités critiques 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 14 Avril 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 14 Avril 2026**:**

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