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 Windows (Patch Tuesday Janvier 2026)
Numéro de Référence	59911501/26
Date de Publication	15 Janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2025 versions antérieures à 10.0.26100.7623
- Windows Server 2025 versions antérieures à 10.0.26100.32230
- Windows Server 2025 (Server Core installation) versions antérieures à 10.0.26100.7623
- Windows Server 2025 (Server Core installation) versions antérieures à 10.0.26100.32230
- Windows Server 2022, 23H2 Edition (Server Core installation) versions antérieures à 10.0.25398.2092
- Windows Server 2022 versions antérieures à 10.0.20348.4648
- Windows Server 2022 (Server Core installation) versions antérieures à 10.0.20348.4648
- Windows Server 2019 versions antérieures à 10.0.17763.8276
- Windows Server 2019 (Server Core installation) versions antérieures à 10.0.17763.8276
- Windows Server 2016 versions antérieures à 10.0.14393.8783
- Windows Server 2016 (Server Core installation) versions antérieures à 10.0.14393.8783
- Windows Server 2012 versions antérieures à 6.2.9200.25868
- Windows Server 2012 R2 versions antérieures à 6.3.9600.22968
- Windows Server 2012 R2 (Server Core installation) versions antérieures à 6.3.9600.22968
- Windows Server 2012 (Server Core installation) versions antérieures à 6.2.9200.25868
- Windows Server 2008 pour systèmes x64 Service Pack 2 versions antérieures à 6.0.6003.23717

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 Server 2008 pour systèmes x64 Service Pack 2 (Server Core installation) versions antérieures à 6.0.6003.23717
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 versions antérieures à 6.0.6003.23717
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (Server Core installation) versions antérieures à 6.0.6003.23717
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 versions antérieures à 6.1.7601.28117
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (Server Core installation) versions antérieures à 6.1.7601.28117
- Windows SDK versions antérieures à 10.0.26100.7463
- Windows Admin Center in Azure Portal versions antérieures à 0.70.0.0
- Windows 11 Version 25H2 pour systèmes x64 versions antérieures à 10.0.26200.7623
- Windows 11 Version 25H2 pour systèmes ARM64 versions antérieures à 10.0.26200.7623
- Windows 11 Version 24H2 pour systèmes x64 versions antérieures à 10.0.26100.7623
- Windows 11 Version 24H2 pour systèmes ARM64 versions antérieures à 10.0.26100.7623
- Windows 11 Version 24H2 pour systèmes ARM64 versions antérieures à 10.0.26100.32230
- Windows 11 Version 23H2 pour systèmes x64 versions antérieures à 10.0.22631.6491
- Windows 11 Version 23H2 pour systèmes ARM64 versions antérieures à 10.0.22631.6491
- Windows 10 Version 22H2 pour systèmes x64 versions antérieures à 10.0.19045.6809
- Windows 10 Version 22H2 pour systèmes ARM64 versions antérieures à 10.0.19045.6809
- Windows 10 Version 22H2 pour systèmes 32 bits versions antérieures à 10.0.19045.6809
- Windows 10 Version 21H2 pour systèmes x64 versions antérieures à 10.0.19044.6809
- Windows 10 Version 21H2 pour systèmes ARM64 versions antérieures à 10.0.19044.6809
- Windows 10 Version 21H2 pour systèmes 32 bits versions antérieures à 10.0.19044.6809
- Windows 10 Version 1809 pour systèmes x64 versions antérieures à 10.0.17763.8276
- Windows 10 Version 1809 pour systèmes 32 bits versions antérieures à 10.0.17763.8276
- Windows 10 Version 1607 pour systèmes x64 versions antérieures à 10.0.14393.8783
- Windows 10 Version 1607 pour systèmes 32 bits versions antérieures à 10.0.14393.8783

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-2023-31096 CVE-2024-55414 CVE-2026-0386 CVE-2026-20804
- CVE-2026-20805 CVE-2026-20808 CVE-2026-20809 CVE-2026-20810
- CVE-2026-20811 CVE-2026-20812 CVE-2026-20814 CVE-2026-20815
- CVE-2026-20816 CVE-2026-20817 CVE-2026-20818 CVE-2026-20819
- CVE-2026-20820 CVE-2026-20821 CVE-2026-20822 CVE-2026-20823
- CVE-2026-20824 CVE-2026-20825 CVE-2026-20826 CVE-2026-20827
- CVE-2026-20828 CVE-2026-20829 CVE-2026-20830 CVE-2026-20831
- CVE-2026-20832 CVE-2026-20833 CVE-2026-20834 CVE-2026-20835
- CVE-2026-20836 CVE-2026-20837 CVE-2026-20838 CVE-2026-20839
- CVE-2026-20840 CVE-2026-20842 CVE-2026-20843 CVE-2026-20844
- CVE-2026-20847 CVE-2026-20848 CVE-2026-20849 CVE-2026-20851
- CVE-2026-20852 CVE-2026-20853 CVE-2026-20854 CVE-2026-20856
- CVE-2026-20857 CVE-2026-20858 CVE-2026-20859 CVE-2026-20860
- CVE-2026-20861 CVE-2026-20862 CVE-2026-20863 CVE-2026-20864
- CVE-2026-20865 CVE-2026-20866 CVE-2026-20867 CVE-2026-20868
- CVE-2026-20869 CVE-2026-20870 CVE-2026-20871 CVE-2026-20872
- CVE-2026-20873 CVE-2026-20874 CVE-2026-20875 CVE-2026-20876
- CVE-2026-20877 CVE-2026-20918 CVE-2026-20919 CVE-2026-20920
- CVE-2026-20921 CVE-2026-20922 CVE-2026-20923 CVE-2026-20924
- CVE-2026-20925 CVE-2026-20926 CVE-2026-20927 CVE-2026-20929
- CVE-2026-20931 CVE-2026-20932 CVE-2026-20934 CVE-2026-20935
- CVE-2026-20936 CVE-2026-20937 CVE-2026-20938 CVE-2026-20939
- CVE-2026-20940 CVE-2026-20941 CVE-2026-20962 CVE-2026-20965
- CVE-2026-21219 CVE-2026-21221 CVE-2026-21265

Bilan de la vulnérabilité

Microsoft a annoncé la correction d'une vulnérabilité critique de type « zero-day », référencée par « CVE-2026-20805» activement exploitée, qui permet à un attaquant de divulguer des informations confidentielles.

En parallèle, l'éditeur a corrigé plusieurs autres vulnérabilités critiques touchant les produits Microsoft Windows concernés. Leur exploitation pourrait offrir à un attaquant la possibilité

d’exécuter du code arbitraire à distance, de provoquer un déni de service (DoS) ou encore de divulguer des informations sensibles.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 13 Janvier 2026**.**

Risque

- Élévation des privilèges ;
- Déni de service ;
- Divulgation d'informations confidentielles ;
- Exécution de code arbitraire à distance ;

Annexe

Bulletin de sécurité Microsoft du 13 Janvier 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