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 Juillet 2025)
Numéro de Référence	55590907/25
Date de Publication	09 Juillet 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows 10 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 21H2 pour x64-based Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 pour 32-bit Systems
- Windows 10 pour x64-based Systems
- Windows Server 2025
- Windows 11 Version 24H2 pour x64-based Systems
- Windows 11 Version 24H2 pour ARM64-based Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 11 Version 23H2 pour x64-based Systems
- Windows Server 2016 (Server Core installation)
- Windows 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

- Windows 11 Version 23H2 pour ARM64-based Systems
- Windows Server 2025 (Server Core installation)
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- Remote Desktop client pour Windows Desktop
- Windows App Client pour Windows Desktop
- Windows Server 2008 pour x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour x64-based Systems Service Pack 2
- Windows Server 2008 pour 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour 32-bit Systems Service Pack 2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1

Identificateurs externes

- CVE-2025-26636 CVE-2025-33054 CVE-2025-36350
- CVE-2025-36357 CVE-2025-47159 CVE-2025-47178
- CVE-2025-47971 CVE-2025-47972 CVE-2025-47973
- CVE-2025-47975 CVE-2025-47976 CVE-2025-47978
- CVE-2025-47980 CVE-2025-47981 CVE-2025-47982
- CVE-2025-47984 CVE-2025-47985 CVE-2025-47986
- CVE-2025-47987 CVE-2025-47991 CVE-2025-47993
- CVE-2025-47994 CVE-2025-47996 CVE-2025-47998
- CVE-2025-47999 CVE-2025-48000 CVE-2025-48001
- CVE-2025-48002 CVE-2025-48003 CVE-2025-48800
- CVE-2025-48802 CVE-2025-48803 CVE-2025-48804
- CVE-2025-48805 CVE-2025-48806 CVE-2025-48808
- CVE-2025-48809 CVE-2025-48810 CVE-2025-48811

- CVE-2025-48812 CVE-2025-48814 CVE-2025-48815
- CVE-2025-48816 CVE-2025-48817 CVE-2025-48818
- CVE-2025-48819 CVE-2025-48820 CVE-2025-48821
- CVE-2025-48822 CVE-2025-48823 CVE-2025-48824
- CVE-2025-48799 CVE-2025-49657 CVE-2025-49658
- CVE-2025-49659 CVE-2025-49660 CVE-2025-49661
- CVE-2025-49663 CVE-2025-49664 CVE-2025-49665
- CVE-2025-49666 CVE-2025-49667 CVE-2025-49668
- CVE-2025-49669 CVE-2025-49670 CVE-2025-49671
- CVE-2025-49672 CVE-2025-49673 CVE-2025-49674
- CVE-2025-49675 CVE-2025-49676 CVE-2025-49677
- CVE-2025-49678 CVE-2025-49679 CVE-2025-49680
- CVE-2025-49681 CVE-2025-49682 CVE-2025-49683
- CVE-2025-49684 CVE-2025-49685 CVE-2025-49686
- CVE-2025-49687 CVE-2025-49688 CVE-2025-49689
- CVE-2025-49690 CVE-2025-49691 CVE-2025-49693
- CVE-2025-49694 CVE-2025-49695 CVE-2025-49696
- CVE-2025-49697 CVE-2025-49698 CVE-2025-49699
- CVE-2025-49700 CVE-2025-49701 CVE-2025-49702
- CVE-2025-49703 CVE-2025-49704 CVE-2025-49705
- CVE-2025-49706 CVE-2025-49711 CVE-2025-49716
- CVE-2025-49721 CVE-2025-49722 CVE-2025-49723
- CVE-2025-49724 CVE-2025-49725 CVE-2025-49726
- CVE-2025-49727 CVE-2025-49729 CVE-2025-49730
- CVE-2025-49731 CVE-2025-49732 CVE-2025-49733
- CVE-2025-49735 CVE-2025-49737 CVE-2025-49738
- CVE-2025-49740 CVE-2025-49742 CVE-2025-49744
- CVE-2025-49753 CVE-2025-49756 CVE-2025-49760

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft Windows. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de réussir une usurpation d'identité, de causer un déni de service, de réussir une élévation de privilèges ou de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 08 Juillet 2025**.**

Risque

- Exécution du code arbitraire à distance
- Contournement de la politique de sécurité
- Déni de service
- Elévation de privilèges
- Usurpation d'identité

Annexe

Bulletin de sécurité Microsoft du 08 Juillet 2025**:**

- 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