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 Septembre 2025)
Numéro de Référence	56661009/25
Date de Publication	10 Septembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2025 (Server Core installation) version 10.0.26100.6584
- Windows Server 2025 (Server Core installation) version 10.0.26100.6508
- Windows 10 Version 1607 pour 32-bit Systems version 10.0.14393.8422
- Windows Server 2025 version 10.0.26100.6584
- Windows Server 2025 version 10.0.26100.6508
- Windows 11 Version 24H2 pour x64-based Systems version 10.0.26100.6584
- Windows 11 Version 24H2 pour x64-based Systems version 10.0.26100.6508
- Windows 11 Version 24H2 pour ARM64-based Systems version 10.0.26100.6584
- Windows 11 Version 24H2 pour ARM64-based Systems version 10.0.26100.6508
- Windows Server 2022, 23H2 Edition (Server Core installation) version 10.0.25398.1849
- Windows 10 Version 1809 pour 32-bit Systems version 10.0.17763.7792
- Windows Server 2016 (Server Core installation) version 10.0.14393.8422
- Windows Server 2016 version 10.0.14393.8422
- Windows 10 Version 1607 pour x64-based Systems version 10.0.14393.8422
- Windows 10 pour x64-based Systems version 10.0.10240.21128
- Windows 10 pour 32-bit Systems version 10.0.10240.21128
- Windows Server 2019 (Server Core installation) version 10.0.17763.7792
- Windows Server 2019 version 10.0.17763.7792
- Windows 10 Version 1809 pour x64-based Systems version 10.0.17763.7792
- Windows Server 2022 version 10.0.20348.4171

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 2022 version 10.0.20348.4106
- 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
- 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

Identificateurs externes

- CVE-2025-54107 CVE-2025-54098 CVE-2025-53803
- CVE-2025-54096 CVE-2025-55234 CVE-2025-54917
- CVE-2025-54915 CVE-2025-54912 CVE-2025-54911
- CVE-2025-54113 CVE-2025-54109 CVE-2025-54104
- CVE-2025-54094 CVE-2025-54093 CVE-2025-54091
- CVE-2025-53810 CVE-2025-53808 CVE-2025-53806
- CVE-2025-53804 CVE-2025-53799 CVE-2025-53796
- CVE-2025-55226 CVE-2025-55225 CVE-2025-54918
- CVE-2025-54916 CVE-2025-54895 CVE-2025-54894
- CVE-2025-54110 CVE-2025-54106 CVE-2025-54101
- CVE-2025-54099 CVE-2025-54097 CVE-2025-54095
- CVE-2025-53798 CVE-2025-53797 CVE-2025-54114
- CVE-2025-54108 CVE-2025-54092 CVE-2025-55236
- CVE-2025-55228 CVE-2025-54919 CVE-2025-54913
- CVE-2025-54102 CVE-2025-55224 CVE-2025-54116
- CVE-2025-54115 CVE-2025-54112 CVE-2025-54105
- CVE-2025-54103 CVE-2025-53809 CVE-2025-53807
- CVE-2025-53805 CVE-2025-53802 CVE-2025-53801
- CVE-2025-53800 CVE-2025-55223 CVE-2025-54111
- CVE-2025-49734

Bilan de la vulnérabilité

Microsoft a annoncé la correction d'une vulnérabilité Zero-Day critique, référencée par « CVE-2025-55234 », affectant les serveurs SMB. Son exploitation réussie pourrait permettre à un attaquant de mener des attaques de relais et d'obtenir une élévation de privilèges.

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), de divulguer des informations sensibles ou encore de contourner certaines fonctionnalités de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 09 Septembre 2025**.**

Risque

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

Annexe

Bulletin de sécurité Microsoft du 09 Septembre 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