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 Novembre 2025)
Numéro de Référence	58281211/25
Date de Publication	12 Novembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows 10 Version 1607 pour 32-bit Systems
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Windows 10 Version 21H2 pour x64-based Systems
- 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 10 pour 32-bit Systems
- Windows 10 pour x64-based Systems
- Windows 11 Version 22H2 pour ARM64-based Systems
- Windows 11 Version 22H2 pour x64-based Systems
- Windows 11 Version 23H2 pour ARM64-based Systems
- Windows 11 Version 23H2 pour x64-based Systems
- Windows 11 Version 24H2 pour ARM64-based Systems
- Windows 11 Version 24H2 pour x64-based Systems
- Windows 11 Version 25H2 pour ARM64-based Systems
- Windows 11 Version 25H2 pour x64-based Systems

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 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows Server 2022 (Server Core installation)
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows Server 2025
- Windows Server 2025 (Server Core installation)
- Windows Server 2012 R2 (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
- 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)

Identificateurs externes

- CVE-2025-62213 CVE-2025-60724 CVE-2025-60704 CVE-2025-60720
- CVE-2025-60715 CVE-2025-60714 CVE-2025-59514 CVE-2025-62452
- CVE-2025-62217 CVE-2025-60719 CVE-2025-60709 CVE-2025-60705
- CVE-2025-60703 CVE-2025-59513 CVE-2025-59512 CVE-2025-59510
- CVE-2025-59506 CVE-2025-59505 CVE-2025-62209 CVE-2025-62208
- CVE-2025-60717 CVE-2025-60716 CVE-2025-60713 CVE-2025-59515
- CVE-2025-62219 CVE-2025-60708 CVE-2025-59508 CVE-2025-60721
- CVE-2025-62215 CVE-2025-60723 CVE-2025-60718 CVE-2025-62218
- CVE-2025-60710 CVE-2025-60707 CVE-2025-60706 CVE-2025-59511
- CVE-2025-59509 CVE-2025-59507

Bilan de la vulnérabilité

Microsoft a annoncé la correction d'une vulnérabilité critique de type « zero-day », référencée par « CVE-2025-62215», une vulnérabilité d'élévation de privilèges dans le noyau Windows.

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 11 Novembre 2025**.**

Risque

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

Annexe

Bulletin de sécurité Microsoft du 11 Novembre 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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma