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 Octobre 2025)
Numéro de Référence	57441510/25
Date de Publication	15 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows 11 Version 25H2 pour ARM64-based Systems 10.0.26200.6899
- Windows 11 Version 25H2 pour x64-based Systems 10.0.26200.6899
- Windows Server 2016 (Server Core installation) 10.0.14393.8519
- Windows Server 2016 10.0.14393.8519
- Windows 10 Version 1607 pour x64-based Systems 10.0.14393.8519
- Windows 10 Version 1607 pour 32-bit Systems 10.0.14393.8519
- Windows 10 pour x64-based Systems 10.0.10240.21161
- Windows 11 Version 23H2 pour x64-based Systems 10.0.22631.6060
- Windows 11 Version 23H2 pour ARM64-based Systems 10.0.22631.6060
- Windows Server 2025 (Server Core installation) 10.0.26100.6899
- Windows 10 Version 22H2 pour 32-bit Systems 10.0.19045.6456
- Windows 10 Version 22H2 pour ARM64-based Systems 10.0.19045.6456
- Windows 10 Version 22H2 pour x64-based Systems 10.0.19045.6456
- Windows 11 Version 22H2 pour x64-based Systems 10.0.22621.6060
- Windows 11 Version 22H2 pour ARM64-based Systems 10.0.22621.6060
- Windows 10 Version 21H2 pour x64-based Systems 10.0.19044.6456
- Windows 10 pour 32-bit Systems 10.0.10240.21161
- Windows Server 2025 10.0.26100.6899
- Windows Server 2019 10.0.17763.7919
- Windows 10 Version 1809 pour x64-based Systems 10.0.17763.7919

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 10 Version 1809 pour 32-bit Systems 10.0.17763.7919
- Windows 11 Version 24H2 pour x64-based Systems 10.0.26100.6899
- Windows 11 Version 24H2 pour ARM64-based Systems 10.0.26100.6899
- Windows Server 2022, 23H2 Edition (Server Core installation) 10.0.25398.1913
- Windows Server 2019 (Server Core installation) 10.0.17763.7919
- Windows 10 Version 21H2 pour ARM64-based Systems 10.0.19044.6456
- Windows 10 Version 21H2 pour 32-bit Systems 10.0.19044.6456
- Windows Server 2022 (Server Core installation) 10.0.20348.4294
- Windows Server 2022 10.0.20348.4294
- Windows Server 2025 10.0.26100.6584
- Windows Server 2025 10.0.26100.6508
- Windows 11 Version 24H2 pour x64-based Systems 10.0.26100.6584
- Windows 11 Version 24H2 pour x64-based Systems 10.0.26100.6508
- Windows 11 Version 24H2 pour ARM64-based Systems 10.0.26100.6584
- Windows 11 Version 24H2 pour ARM64-based Systems 10.0.26100.6508
- Windows Server 2022, 23H2 Edition (Server Core installation) 10.0.25398.1849
- Windows 11 Version 23H2 pour x64-based Systems 10.0.22631.5909
- Windows 11 Version 23H2 pour ARM64-based Systems 10.0.22631.5909
- Windows Server 2025 (Server Core installation) 10.0.26100.6584
- Windows Server 2025 (Server Core installation) 10.0.26100.6508
- Windows 10 Version 22H2 pour 32-bit Systems 10.0.19044.6332
- Windows 10 Version 22H2 pour ARM64-based Systems 10.0.19044.6332
- Windows 10 Version 22H2 pour x64-based Systems 10.0.19044.6332
- Windows 11 Version 22H2 pour x64-based Systems 10.0.22631.5909
- Windows 11 Version 22H2 pour ARM64-based Systems 10.0.22631.5909
- Windows 10 Version 21H2 pour x64-based Systems 10.0.19044.6332
- Windows 10 Version 21H2 pour ARM64-based Systems 10.0.19044.6332
- Windows 10 Version 21H2 pour 32-bit Systems 10.0.19044.6332
- Windows Server 2022 (Server Core installation) 10.0.20348.4171
- Windows Server 2022 (Server Core installation) 10.0.20348.4106
- Windows Server 2022 10.0.20348.4171
- Windows Server 2022 10.0.20348.4106
- Remote Desktop client pour Windows Desktop 1.2.6599.0

- Windows App Client pour Windows Desktop 2.0.706.0
- Windows Server 2019 (Server Core installation) 10.0.17763.7792
- Windows Server 2019 10.0.17763.7792
- Windows 10 Version 1809 pour x64-based Systems 10.0.17763.7792
- Windows 10 Version 1809 pour 32-bit Systems 10.0.17763.7792
- 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 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 2012
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)

Identificateurs externes

- CVE-2025-59502 CVE-2025-59295 CVE-2025-59294 CVE-2025-59295
- CVE-2025-59287 CVE-2025-59194 CVE-2025-59189 CVE-2025-59287
- CVE-2025-59284 CVE-2025-59282 CVE-2025-47979 CVE-2025-59282
- CVE-2025-59280 CVE-2025-54957 CVE-2025-49708 CVE-2025-59280
- CVE-2025-59278 CVE-2025-59277 CVE-2025-59259 CVE-2025-59258
- CVE-2025-59277 CVE-2025-59275 CVE-2025-59260 CVE-2025-58730
- CVE-2025-58727 CVE-2025-59259 CVE-2025-59258 CVE-2025-59257
- CVE-2025-59255 CVE-2025-59254 CVE-2025-59253 CVE-2025-59244
- CVE-2025-2884 CVE-2025-59241 CVE-2025-59244 CVE-2025-59242
- CVE-2025-59211 CVE-2025-59207 CVE-2025-59242 CVE-2025-59230
- CVE-2025-59192 CVE-2025-59275 CVE-2025-59230 CVE-2025-59214
- CVE-2025-59211 CVE-2025-59209 CVE-2025-59208 CVE-2025-59278
- CVE-2025-59209 CVE-2025-59208 CVE-2025-59206 CVE-2025-59202
- CVE-2025-59201 CVE-2025-59205 CVE-2025-59203 CVE-2025-59190
- CVE-2025-59205 CVE-2025-59204 CVE-2025-59200 CVE-2025-59199
- CVE-2025-59202 CVE-2025-59201 CVE-2025-59198 CVE-2025-59197

- CVE-2025-59289 CVE-2025-59198 CVE-2025-59196 CVE-2025-59195
- CVE-2025-59186 CVE-2025-59196 CVE-2025-59191 CVE-2025-59214
- CVE-2025-59210 CVE-2025-59190 CVE-2025-59188 CVE-2025-59184
- CVE-2025-58734 CVE-2025-59188 CVE-2025-59187 CVE-2025-58737
- CVE-2025-58736 CVE-2025-59187 CVE-2025-59185 CVE-2025-58732
- CVE-2025-58728 CVE-2025-59185 CVE-2025-58739 CVE-2025-59261
- CVE-2025-59253 CVE-2025-58739 CVE-2025-58738 CVE-2025-47827
- CVE-2025-59193 CVE-2025-58737 CVE-2025-58736 CVE-2025-58735
- CVE-2025-58722 CVE-2025-58719 CVE-2025-58735 CVE-2025-58733
- CVE-2025-58731 CVE-2025-58729 CVE-2025-58733 CVE-2025-58732
- CVE-2025-58730 CVE-2025-58729 CVE-2025-58726 CVE-2025-58720
- CVE-2025-58718 CVE-2025-58726 CVE-2025-58725 CVE-2025-58714
- CVE-2025-55695 CVE-2025-58725 CVE-2025-58718 CVE-2025-58717
- CVE-2025-58716 CVE-2025-55701 CVE-2025-58717 CVE-2025-58715
- CVE-2025-55700 CVE-2025-55689 CVE-2025-58714 CVE-2025-55701
- CVE-2025-55700 CVE-2025-55699 CVE-2025-55698 CVE-2025-55697
- CVE-2025-55696 CVE-2025-55694 CVE-2025-55693 CVE-2025-55695
- CVE-2025-55692 CVE-2025-55691 CVE-2025-55690 CVE-2025-55692
- CVE-2025-55688 CVE-2025-55684 CVE-2025-55683 CVE-2025-55687
- CVE-2025-55686 CVE-2025-55685 CVE-2025-55687 CVE-2025-55682
- CVE-2025-55680 CVE-2025-55332 CVE-2025-55681 CVE-2025-55336
- CVE-2025-55325 CVE-2025-55679 CVE-2025-55678 CVE-2025-55337
- CVE-2025-55339 CVE-2025-55338 CVE-2025-55335 CVE-2025-55677
- CVE-2025-55676 CVE-2025-55340 CVE-2025-55678 CVE-2025-50174
- CVE-2025-48004 CVE-2025-50175 CVE-2025-53150 CVE-2025-50152
- CVE-2025-53139 CVE-2016-9535 CVE-2025-59290 CVE-2025-53717
- CVE-2025-25004 CVE-2025-48813 CVE-2025-55328 CVE-2025-55326
- CVE-2025-53768 CVE-2025-55333 CVE-2025-24052 CVE-2025-24990
- CVE-2025-55334 CVE-2025-55331 CVE-2025-55330 CVE-2025-55335
- CVE-2025-47827 CVE-2025-25004 CVE-2025-24990 CVE-2025-24052
- CVE-2016-9535

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

Bilan de la vulnérabilité

Microsoft a publié des correctifs de sécurité pour des vulnérabilités critiques de type zero-day affectant les versions susmentionnées des systèmes d'exploitation Windows. Quatre de ces vulnérabilités ont été activement exploitées avant la publication des correctifs :

- **CVE-2025-24990 :** Cette faille permet à un attaquant d'obtenir les droits administrateur sur un système Windows en utilisant un ancien pilote de modem nommé « ltmdm64.sys », installé par défaut sur plusieurs versions de Windows.
- **CVE-2025-24052** : Il s'agit d'une autre vulnérabilité liée au même pilote « ltmdm64.sys ». Elle permet également une élévation de privilèges. Microsoft précise que toutes les versions de Windows sont vulnérables.
- **CVE-2025-59230 :** Cette vulnérabilité affecte le service Windows de gestion des connexions à distance. Elle permet à un utilisateur local autorisé de passer à des privilèges « SYSTEM », ce qui donne un contrôle total sur l'ordinateur.
- **CVE-2025-47827 :** Ce bug affecte « IGEL OS » (avant la version 11), un système utilisé dans certains environnements Windows. Il permet à un attaquant de contourner la vérification de « Secure Boot » en chargeant un système modifié non sécurisé au démarrage.

En parallèle, l'éditeur a corrigé plusieurs autres vulnérabilités critiques, 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 14 Octobre 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 14 Octobre 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