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 dans Microsoft Windows (Patch Tuesday Octobre 2024)
Numéro de Référence	50020910/24
Date de Publication	09 Octobre 2024
Risque	Important
Impact	Important

Systèmes affectés

- 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 11 version 21H2 pour ARM64-based Systems
- Windows 11 version 21H2 pour x64-based Systems
- Windows Server 2016
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- Windows 10 pour x64-based Systems
- Windows 10 pour 32-bit Systems
- Windows 11 Version 24H2 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 Server 2022, 23H2 Edition (Server Core installation)
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 11 Version 24H2 pour ARM64-based Systems

- Windows 11 Version 23H2 pour x64-based Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows Server 2016 (Server Core installation)
- Windows 11 Version 23H2 pour ARM64-based Systems
- Remote Desktop client pour Windows Desktop
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 pour 32-bit Systems Service Pack 2
- Windows Server 2008 pour 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour x64-based Systems Service Pack 2
- Windows Server 2008 pour x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)

Identificateurs externes

- CVE-2024-43573 CVE-2024-43611 CVE-2024-43583 CVE-2024-43593 CVE-2024-43592 CVE-2024-43589 CVE-2024-43585 CVE-2024-43584 CVE-2024-43575 CVE-2024-43574 CVE-2024-43571 CVE-2024-43570 CVE-2024-43567 CVE-2024-43565 CVE-2024-43564 CVE-2024-43563 CVE-2024-43562 CVE-2024-43561 CVE-2024-43560 CVE-2024-43559 CVE-2024-43558 CVE-2024-43557 CVE-2024-43556 CVE-2024-43555 CVE-2024-43553 CVE-2024-43552 CVE-2024-43551 CVE-2024-43550 CVE-2024-43549 CVE-2024-43547 CVE-2024-43546 CVE-2024-43545 CVE-2024-43536 CVE-2024-43528 CVE-2024-43524 CVE-2024-43523 CVE-2024-43522 CVE-2024-43521 CVE-2024-43520 CVE-2024-43514 CVE-2024-43512 CVE-2024-43511 CVE-2024-43509 CVE-2024-43501 CVE-2024-43456 CVE-2024-30092 CVE-2024-38212 CVE-2024-43453 CVE-2024-38262 CVE-2024-38265 CVE-2024-38124 CVE-2024-38129 CVE-2024-38029 CVE-2024-37983 CVE-2024-37979 CVE-2024-37982 CVE-2024-37976 CVE-2024-20659 CVE-2024-43500 CVE-2024-43615 CVE-2024-43607 CVE-2024-43609 CVE-2024-43608 CVE-2024-6197 CVE-2024-43581 CVE-2024-43554 CVE-2024-43543 CVE-2024-43542 CVE-2024-43540 CVE-2024-43538 CVE-2024-43537 CVE-2024-43535 CVE-2024-43534 CVE-2024-43529 CVE-2024-43527 CVE-2024-43526 CVE-2024-43525 CVE-2024-43518 CVE-2024-43513 CVE-2024-43508 CVE-2024-43502 CVE-2024-38261 CVE-2024-43516 CVE-2024-37341 CVE-2022-0001 CVE-2021-1638 CVE-2021-1684 CVE-2021-1683 CVE-2024-43582 ADV990001

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les systèmes d'exploitation Windows susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de divulguer des informations confidentielles, d'exécuter du code arbitraire, réussir une élévation de privilèges, de causer un déni de service et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 08 Octobre 2024**.**

Risque

- Déni de service
- Exécution de code à distance
- Élévation du privilège
- Divulgation d'informations
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Microsoft du 08 Octobre 2024**:**

- https://msrc.microsoft.com/update-guide/