



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Microsoft Windows (Patch Tuesday Novembre 2024)
Numéro de Référence	50761311/24
Date de Publication	13 Novembre 2024
Risque	Critique
Impact	Critique

Systemes affectés

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

- Windows 11 Version 24H2 pour ARM64-based Systems
- Windows 11 Version 23H2 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 Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 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-2024-43639 CVE-2024-43629 CVE-2024-43624 CVE-2024-43451
- CVE-2024-43450 CVE-2024-43644 CVE-2024-43637 CVE-2024-43630
- CVE-2024-43628 CVE-2024-43626 CVE-2024-49039 CVE-2024-49019
- CVE-2024-38203 CVE-2024-43642 CVE-2024-43641 CVE-2024-43640
- CVE-2024-43636 CVE-2024-43635 CVE-2024-43633 CVE-2024-43622
- CVE-2024-43621 CVE-2024-43620 CVE-2024-49046 CVE-2024-38264
- CVE-2024-43452 CVE-2024-43449 CVE-2024-43447 CVE-2024-43646
- CVE-2024-43645 CVE-2024-43643 CVE-2024-43638 CVE-2024-43634
- CVE-2024-43631 CVE-2024-43627 CVE-2024-43625 CVE-2024-43623
- CVE-2024-43530

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, réussir une élévation de privilèges, une usurpation d'identité, de causer un déni de service et de contourner la politique de sécurité.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 12 Novembre 2024.

Risque

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

Annexe

Bulletin de sécurité Microsoft du 12 Novembre 2024:

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