



BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans Microsoft Windows (Patch Tuesday Janvier 2024)
<b>Numéro de Référence</b>	45471001/24
<b>Date de Publication</b>	10 Janvier 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

**Systèmes affectés**

- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 11 Version 23H2 pour x64-based Systems
- Windows 11 Version 23H2 pour ARM64-based Systems
- Windows 11 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour ARM64-based Systems
- Windows 11 version 21H2 pour ARM64-based Systems
- Windows 11 version 21H2 pour x64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 10 Version 22H2 pour x64-based Systems
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-based Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 pour ARM64-based Systems
- Windows Server 2016 (Server Core installation)
- 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 10 Version 21H2 pour x64-based Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Microsoft Printer Metadata Troubleshooter Tool
- 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-2024-21309 CVE-2024-20700 CVE-2024-21306 CVE-2022-35737 CVE-2024-20692 CVE-2024-20687 CVE-2024-21310 CVE-2024-20674 CVE-2024-20698 CVE-2024-20696 CVE-2024-20666 CVE-2024-20683 CVE-2024-20660 CVE-2024-21307 CVE-2024-20652 CVE-2024-21320 CVE-2024-20697 CVE-2024-20658 CVE-2024-21314 CVE-2024-21311 CVE-2024-20653 CVE-2024-20694 CVE-2024-21305 CVE-2024-21316 CVE-2024-21313 CVE-2024-20682 CVE-2024-21325 CVE-2024-20699 CVE-2024-20691 CVE-2024-20690 CVE-2024-20686 CVE-2024-20681 CVE-2024-20680 CVE-2024-20664 CVE-2024-20663 CVE-2024-20662 CVE-2024-20661 CVE-2024-20657 CVE-2024-20655 CVE-2024-20654

### Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques dans 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

Veillez se référer au bulletin de sécurité Microsoft du 09 Janvier 2024.

### Risque

- Déni de service

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

## Annexe

Bulletin de sécurité Microsoft du 09 Janvier 2024:

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