



BULLETIN DE SECURITE

| | |
|----------------------------|--|
| Titre | Vulnérabilités critiques dans Microsoft Windows (Patch Tuesday Mai 2023) |
| Numéro de Référence | 41731005/23 |
| Date de Publication | 10 Mai 2023 |
| Risque | Critique |
| Impact | Critique |

Systèmes affectés

- 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 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 10 Version 20H2 pour ARM64-based Systems
- Windows 10 Version 20H2 pour 32-bit Systems
- Windows 10 Version 20H2 pour x64-based Systems
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 pour ARM64-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 Server 2016

- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows 10 pour x64-based Systems
- Windows 10 pour 32-bit Systems
- AV1 Video Extension
- Microsoft Remote Desktop
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

Identificateurs externes

- CVE-2023-24949 , CVE-2023-24947 , CVE-2023-24903 , CVE-2023-29341 , CVE-2023-29340 , CVE-2023-29336 , CVE-2023-29325 , CVE-2023-29324 , CVE-2023-24948 , CVE-2023-24946 , CVE-2023-24945 , CVE-2023-24944 , CVE-2023-24905 , CVE-2023-24943 , CVE-2023-24942 , CVE-2023-24902 , CVE-2023-24941 , CVE-2023-24901 , CVE-2023-24940 , CVE-2023-24900 , CVE-2023-24939 , CVE-2023-24899 , CVE-2023-24898 , CVE-2023-28290 , CVE-2023-28283 , CVE-2023-28251 , CVE-2023-24932 , CVE-2023-29343 , CVE-2023-29338 , CVE-2023-29336 , CVE-2023-29324 , CVE-2023-24946 , CVE-2023-24945 , CVE-2023-24904 , CVE-2023-24942 , CVE-2023-24940 , CVE-2023-24900 , CVE-2023-28251 , CVE-2023-24932 , CVE-2023-24903 , CVE-2023-29325 , CVE-2023-24943 , CVE-2023-28283

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

Veuillez se référer au bulletin de sécurité Microsoft du 09 Mai 2023.

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 Mai 2023:

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