



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant Microsoft Windows (Patch Tuesday Décembre 2022)
Numéro de Référence	39481412/22
Date de Publication	14 Décembre 2021
Risque	Important
Impact	Critique

Systèmes affectés

- Windows Server 2022 Datacenter: Azure Edition
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 10 Version 21H1 for x64-based Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for x64-based Systems
- Windows RT 8.1
- Windows 8.1 for 32-bit systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 for 32-bit Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 for ARM64-based Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 1809 for ARM64-based Systems

- Windows 10 Version 1809 for 32-bit Systems
- Remote Desktop client for Windows Desktop

Identificateurs externes

CVE-2022-44687	CVE-2022-41094	CVE-2022-41076	CVE-2022-44710
CVE-2022-44707	CVE-2022-44698	CVE-2022-44697	CVE-2022-44689
CVE-2022-44683	CVE-2022-44682	CVE-2022-44681	CVE-2022-44680
CVE-2022-44679	CVE-2022-44677	CVE-2022-44678	CVE-2022-44676
CVE-2022-44675	CVE-2022-44674	CVE-2022-44673	CVE-2022-44671
CVE-2022-44670	CVE-2022-44669	CVE-2022-44668	CVE-2022-44667
CVE-2022-44666	CVE-2022-41121	CVE-2022-41077	CVE-2022-41074

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son système d'exploitation Microsoft Windows. Parmi les vulnérabilités corrigées on retrouve deux vulnérabilités « zero-day » identifiées par « CVE-2022-44710 » et « CVE-2022-44698 » dont une est activement exploitée. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'élévation de privilèges, l'exécution de code arbitraire, l'accès à des données confidentielles ou le déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Microsoft pour obtenir les nouvelles mises à jour

Risque

- Elévation de privilèges
- Exécution de code arbitraire
- Accès à des données confidentielles
- Déni de service

Référence

Guide de sécurité de Microsoft :

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