

ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information
.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques



المملكة المغربية
ادارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي
للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant Microsoft Windows (Patch Tuesday Décembre 2023)
Numéro de Référence	45141312/23
Date de Publication	13 Décembre 2023
Risque	Important
Impact	Critique

Systèmes affectés

- 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 Server 2016 (Server Core installation)
- Windows Server 2016
- Windows 11 version 21H2 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems

- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems

Identificateurs externes

CVE-2023-35634 CVE-2023-35644 CVE-2023-36696 CVE-2023-35631
CVE-2023-36391 CVE-2023-36003 CVE-2023-35635

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son système d’exploitation Microsoft Windows. L’exploitation de ces vulnérabilités peut permettre à un attaquant l’élévation de privilèges, l’exécution de code arbitraire, ou de causer un 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
- Déni de service

Référence

Guide de sécurité de Microsoft :

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