ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans Microsoft Windows (Patch Tuesday Mars 2024)
Numéro de Référence	46461303/24
Date de Publication	13 Mars 2024
Risque	Important
Impact	Important

Systèmes affectés

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

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Windows 11 version 21H2 pour ARM64-based Systems
- Windows 11 version 21H2 pour x64-based Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 10 Version 21H2 pour x64-based Systems
- Windows Defender Antimalware Platform
- 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-2024-21442 CVE-2024-21437 CVE-2024-21433 CVE-2024-21430 CVE-2024-21429 CVE-2024-26185 CVE-2024-26182 CVE-2024-26177 CVE-2024-26176 CVE-2024-26173 CVE-2024-26166 CVE-2024-26159 CVE-2024-21440 CVE-2024-26161 CVE-2024-21443 CVE-2024-26170 CVE-2024-21451 CVE-2024-26174 CVE-2024-21439 CVE-2024-21438 CVE-2024-26169 CVE-2024-21441 CVE-2024-21435 CVE-2024-26162 CVE-2024-26160 CVE-2024-26190 CVE-2024-26181 CVE-2024-26197 CVE-2024-21446 CVE-2024-21445 CVE-2024-26178 CVE-2023-28746 CVE-2024-21434 CVE-2024-21450 CVE-2024-21444 CVE-2024-21436 CVE-2024-21432 CVE-2024-21431 CVE-2024-21427 CVE-2024-21408 CVE-2024-21407

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités 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 12 Mars 2024**.**

Risque

- Déni de service
- Exécution de code à distance
- Élévation du privilège

- Divulgation d'informations
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Microsoft du 12 Mars 2024**:**

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