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 critiques dans Microsoft Windows (Patch Tuesday Avril 2023)
Numéro de Référence	41301204/23
Date de Publication	12 Avril 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- 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
- Raw Image Extension
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- 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 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
- Remote Desktop client pour Windows Desktop
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1
- Windows Server 2008 pour x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour x64-based Systems Service Pack 2
- Windows Server 2008 pour 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour 32-bit Systems Service Pack 2

Identificateurs externes

- CVE-2023-21729 , CVE-2023-28292 , CVE-2023-28291 , CVE-2023-28308 , CVE-2023-28307 , CVE-2023-28306 , CVE-2023-28305 , CVE-2023-28302 , CVE-2023-28298 , CVE-2023-28297 , CVE-2023-28293 , CVE-2023-28256 , CVE-2023-28278 , CVE-2023-28255 , CVE-2023-28253 , CVE-2023-28254 , CVE-2023-28275 , CVE-2023-28276 , CVE-2023-28252 , CVE-2023-28274 , CVE-2023-28277 , CVE-2023-28250 , CVE-2023-28273 , CVE-2023-28249 , CVE-2023-28272 , CVE-2023-28271 , CVE-2023-28247 , CVE-2023-28248 , CVE-2023-28269 , CVE-2023-28270 , CVE-2023-28246 , CVE-2023-28268 , CVE-2023-28244 , CVE-2023-28266 , CVE-2023-28267 , CVE-2023-28243 , CVE-2023-28241 , CVE-2023-28240 , CVE-2023-28236 , CVE-2023-28238 , CVE-2023-28237 , CVE-2023-28232 , CVE-2023-28235 , CVE-2023-28231 , CVE-2023-28234 , CVE-2023-28233 , CVE-2023-28228 , CVE-2023-28229 , CVE-2023-28227 , CVE-2023-28224 , CVE-2023-28226 , CVE-2023-28225 , CVE-2023-28223 , CVE-2023-28222 , CVE-2023-28221 , CVE-2023-28220 , CVE-2023-28219 , CVE-2023-28218 , CVE-2023-28217 , CVE-2023-28216 , CVE-2023-24931 , CVE-2023-24929 , CVE-2023-24887 , CVE-2023-24928 , CVE-2023-24886 , CVE-2023-24927 , CVE-2023-24885 , CVE-2023-24926 , CVE-2023-24884 , CVE-2023-24925 , CVE-2023-24883 , CVE-2023-24924 , CVE-2023-24914 , CVE-2023-24912 , CVE-2023-21769 , CVE-2023-21727 , CVE-2023-21554

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 12 Avril 2023**.**

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 Avril 2023**:**

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

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma