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 Février 2024)
Numéro de Référence	46011402/24
Date de Publication	14 Février 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- 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 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 1809 pour 32-bit Systems
- Windows 10 pour 32-bit Systems
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 11 Version 23H2 pour x64-based Systems
- Windows 11 Version 23H2 pour ARM64-based Systems
- 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 Server 2022
- Windows 11 version 21H2 pour x64-based Systems
- Windows 10 pour x64-based Systems
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-based 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 10 Version 22H2 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 Server 2022 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 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-2024-21355 CVE-2024-21354 CVE-2024-21349 CVE-2024-21405 CVE-2024-21391 CVE-2024-21412 CVE-2024-21343 CVE-2024-21406 CVE-2024-21366 CVE-2024-21365 CVE-2024-21362 CVE-2024-21361 CVE-2024-21370 CVE-2024-21359 CVE-2024-21356 CVE-2024-21368 CVE-2024-21352 CVE-2024-21351 CVE-2024-21371 CVE-2024-21348 CVE-2024-21358 CVE-2024-21357 CVE-2024-21420 CVE-2024-21375 CVE-2024-21340 CVE-2024-21377 CVE-2024-21360 CVE-2024-21339 CVE-2024-21367 CVE-2024-21353 CVE-2024-20684 CVE-2023-50387 CVE-2024-21304 CVE-2024-21372 CVE-2024-21347 CVE-2024-21350 CVE-2024-21369 CVE-2024-21363 CVE-2024-21346 CVE-2024-21345 CVE-2024-21344 CVE-2024-21342 CVE-2024-21341 CVE-2024-21338

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 13 Février 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 13 Février 2024**:**

- 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