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 Mars 2023)
Numéro de Référence	40831503/23
Date de Publication	15 Mars 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows 11 Version 22H2 pour x64-based Systems
- Windows 10 pour x64-based Systems
- Windows 10 Version 22H2 pour x64-based Systems
- 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 32-bit Systems
- Windows 10 Version 22H2 pour 32-bit Systems
- Windows 10 Version 22H2 pour ARM64-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
- Windows 10 Version 20H2 pour ARM64-based Systems
- Windows 10 Version 20H2 pour 32-bit Systems
- Windows Server 2022 (Server Core installation)

- Windows Server 2022
- Windows 10 Version 20H2 pour x64-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 10 Version 1809 pour 32-bit Systems
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2

Identificateurs externes

- CVE-2023-23392 , CVE-2023-1018 , CVE-2023-24911 , CVE-2023-24870 , CVE-2023-24880 , CVE-2023-24876 , CVE-2023-24908 , CVE-2023-24910 , CVE-2023-24909 , CVE-2023-24868 , CVE-2023-24872 , CVE-2023-23403 , CVE-2023-24871 , CVE-2023-24869 , CVE-2023-24907 , CVE-2023-1017 , CVE-2023-24913 , CVE-2023-24867 , CVE-2023-24906 , CVE-2023-24866 , CVE-2023-24865 , CVE-2023-24864 , CVE-2023-24863 , CVE-2023-24862 , CVE-2023-24861 , CVE-2023-24859 , CVE-2023-24858 , CVE-2023-24857 , CVE-2023-24856 , CVE-2023-23423 , CVE-2023-23422 , CVE-2023-23421 , CVE-2023-23420 , CVE-2023-23419 , CVE-2023-23418 , CVE-2023-23417 , CVE-2023-23416 , CVE-2023-23415 , CVE-2023-23414 , CVE-2023-23413 , CVE-2023-23412 , CVE-2023-23411 , CVE-2023-23410 , CVE-2023-23409 , CVE-2023-23407 , CVE-2023-23406 , CVE-2023-23405 , CVE-2023-23404 , CVE-2023-23402 , CVE-2023-23401 , CVE-2023-23400 , CVE-2023-23394 , CVE-2023-23393 , CVE-2023-23388 , CVE-2023-23385 , CVE-2023-21708

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques dans les systèmes d'exploitation Windows susmentionnés. Selon Microsoft une de ces vulnérabilités identifiée par «CVE-2023-24880 » est activement exploitée.

Microsoft confirme qu'un attaquant peut créer un fichier malveillant qui échappe aux défenses MOTW (Mark of the Web), ce qui entraîne une perte de l'intégrité et de la disponibilité des fonctions de sécurité telles que « Protected View » dans Microsoft Office, qui s'appuient sur le marquage MOTW.

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 14 Mars 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 14 Mars 2023**:**

- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880