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 2023)
Numéro de Référence	40281502/23
Date de Publication	15 Février 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- 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
- Windows 10 Version 20H2 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 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
- 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-2023-21823 CVE-2023-23376 CVE-2023-21805 CVE-2023-21702 CVE-2023-21701 CVE-2023-21700 CVE-2023-21699 CVE-2023-21697 CVE-2023-21695 CVE-2023-21694 CVE-2023-21693 CVE-2023-21692 CVE-2023-21691 CVE-2023-21690 CVE-2023-21689 CVE-2023-21688 CVE-2023-21687 CVE-2023-21686 CVE-2023-21685 CVE-2023-21822 CVE-2023-21820 CVE-2023-21818 CVE-2023-21817 CVE-2023-21816 CVE-2023-21819 CVE-2023-21813 CVE-2023-21812 CVE-2023-21811 CVE-2023-21804 CVE-2023-21803 CVE-2023-21802 CVE-2023-21801 CVE-2023-21799 CVE-2023-21798 CVE-2023-21797 CVE-2023-21684

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques dans les systèmes d'exploitation Windows susmentionnés. Selon Microsoft deux de ces vulnérabilités identifiées par «CVE-2023-23376 et CVE-2023-21823 » sont des « Zero-day » et peuvent permettre à un attaquant d'exécuter du code arbitraire. 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 et de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 14 Février 2023**.**

Risque

- Déni de service

- Exécution de code à distance
- Élévation du privilège
- Divulgation d'informations

Annexe

Bulletin de sécurité Microsoft du 14 Février 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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma