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 Janvier 2023)
Numéro de Référence	39681201/23
Date de Publication	12 Janvier 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows 10 Version 1607 pour systèmes 32 bits
- Windows 10 Version 1607 pour systèmes x64
- Windows 10 Version 1809 pour systèmes 32 bits
- Windows 10 Version 1809 pour systèmes ARM64
- Windows 10 Version 1809 pour systèmes x64
- Windows 10 Version 20H2 pour systèmes 32 bits
- Windows 10 Version 20H2 pour systèmes ARM64
- Windows 10 Version 20H2 pour systèmes x64
- Windows 10 Version 21H2 pour systèmes 32 bits
- Windows 10 Version 21H2 pour systèmes ARM64
- Windows 10 Version 21H2 pour systèmes x64
- Windows 10 Version 22H2 pour systèmes 32 bits
- Windows 10 Version 22H2 pour systèmes ARM64
- Windows 10 Version 22H2 pour systèmes x64
- Windows 10 pour systèmes 32 bits
- Windows 10 pour systèmes x64
- Windows 11 Version 22H2 pour systèmes ARM64
- Windows 11 Version 22H2 pour systèmes x64
- Windows 11 version 21H2 pour systèmes ARM64
- Windows 11 version 21H2 pour systèmes x64
- Windows 7 pour systèmes 32 bits Service Pack 1

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 7 pour systèmes x64 Service Pack 1
- Windows 8.1 pour systèmes 32 bits
- Windows 8.1 pour systèmes x64
- Windows Malicious Software Removal Tool 32 bits
- Windows Malicious Software Removal Tool 64 bits
- Windows RT 8.1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (Server Core installation)
- Windows Server 2008 pour systèmes 32 bits Service Pack 2
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (Server Core installation)
- Windows Server 2008 pour systèmes x64 Service Pack 2
- Windows Server 2008 pour systèmes x64 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)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows Server 2022 (Server Core installation)

Identificateurs externes

- CVE-2023-21541 , CVE-2023-21776 , CVE-2023-21754 , CVE-2023-21753 , CVE-2023-21750 , CVE-2023-21749 , CVE-2023-21748 , CVE-2023-21739 , CVE-2023-21730 , CVE-2023-21681 , CVE-2023-21682 , CVE-2023-21679 , CVE-2023-21677 , CVE-2023-21675 , CVE-2023-21558 , CVE-2023-21557 , CVE-2023-21543 , CVE-2023-21676 , CVE-2023-21549 , CVE-2023-21548 , CVE-2023-21728 , CVE-2023-21773 , CVE-2023-21758 , CVE-2023-21678 , CVE-2023-21772 , CVE-2023-21771 , CVE-2023-21752 , CVE-2023-21760 , CVE-2023-21726 , CVE-2023-21556 , CVE-2023-21551 , CVE-2023-21550 , CVE-2023-21767 , CVE-2023-21759 , CVE-2023-21563 , CVE-2023-21766 , CVE-2023-21733 , CVE-2023-21732 , CVE-2023-21724 , CVE-2023-21540 , CVE-2023-21774 , CVE-2023-21757 , CVE-2023-21539 , CVE-2023-21524 , CVE-2023-21747 , CVE-2023-21680 , CVE-2023-21560 , CVE-2023-21555 , CVE-2023-21552 , CVE-2023-21525 , CVE-2023-21546 , CVE-2023-21768 , CVE-2023-21746 , CVE-2023-21725 , CVE-2023-21559 , CVE-2023-21765 , CVE-2023-21561 , CVE-2023-21683 , CVE-2023-21527 , CVE-2023-21755 , CVE-2023-

21674 , CVE-2023-21542 , CVE-2023-21547 , CVE-2023-21537 , CVE-2023-21536 , CVE-2023-21535 , CVE-2023-21532

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, exécuter du code arbitraire, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou de réussir une usurpation d'identité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 10 janvier 2023**.**

Risque

- Déni de service ;
- Exécution de code à distance ;
- Élévation du privilège ;
- Divulgation d'informations ;
- Contournement de la politique de sécurité ;
- Usurpation d'identité ;

Annexe

Bulletin de sécurité Microsoft du 10 janvier 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