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 Novembre 2022)
Numéro de Référence	39070911/22
Date de Publication	09 Novembre 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2022 Datacenter: Azure Edition (Hotpatch)
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server 2016 (Server Core installation)
- Windows Server 2016
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012
- Windows RT 8.1
- Windows 8.1 pour x64-based systems
- Windows 8.1 pour 32-bit systems
- Windows 11 pour x64-based Systems
- Windows 11 pour ARM64-based Systems
- Windows 11 Version 22H2 pour x64-based Systems
- Windows 11 Version 22H2 pour ARM64-based Systems
- Windows 10 pour x64-based Systems
- Windows 10 pour 32-bit Systems
- Windows 10 Version 22H2 pour x64-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 ARM64-based Systems
- Windows 10 Version 22H2 pour 32-bit 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 10 Version 21H1 pour x64-based Systems
- Windows 10 Version 21H1 pour ARM64-based Systems
- Windows 10 Version 21H1 pour 32-bit Systems
- Windows 10 Version 20H2 pour x64-based Systems
- Windows 10 Version 20H2 pour ARM64-based Systems
- Windows 10 Version 20H2 pour 32-bit Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 1809 pour ARM64-based Systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 10 Version 1607 pour x64-based Systems
- Windows 10 Version 1607 pour 32-bit Systems
- 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
- 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 7 pour x64-based Systems Service Pack 1
- Windows 7 pour 32-bit Systems Service Pack 1

Identificateurs externes

- CVE-2022-41098 CVE-2022-41056 CVE-2022-41100 CVE-2022-41086 CVE-2022-41125 CVE-2022-41092 CVE-2022-41055 CVE-2022-41053 CVE-2022-41090 CVE-2022-41058 CVE-2022-37992 CVE-2022-41114 CVE-2022-41039 CVE-2022-41109 CVE-2022-41057 CVE-2022-38015 CVE-2022-41054 CVE-2022-41113 CVE-2022-41102 CVE-2022-41050 CVE-2022-41049 CVE-2022-41091 CVE-2022-41052 CVE-2022-37967 CVE-2022-23824 CVE-2022-41096 CVE-2022-38023 CVE-2022-37966 CVE-2022-41095 CVE-2022-41128 CVE-2022-41118 CVE-2022-41099 CVE-2022-41073

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques et quatre zero-day activement exploités affectant les systèmes d'exploitation Windows susmentionnés. Les vulnérabilités zero-day corrigées sont :

- CVE-2022-41128 - Vulnérabilité d'exécution de code à distance des langages de script de Windows.
- CVE-2022-41091 - Vulnérabilité de contournement de la fonction de sécurité Mark of the Web (MOTW) de Windows
- CVE-2022-41073 - Vulnérabilité d'élévation de privilège de Windows Print Spooler. Un attaquant ayant réussi à exploiter cette vulnérabilité pourrait obtenir des privilèges SYSTEM".
- CVE-2022-41125 - Vulnérabilité d'élévation de privilège du service d'isolation des clés de Windows CNG. Un attaquant ayant réussi à exploiter cette vulnérabilité pourrait obtenir des privilèges SYSTEM.

En revanche, l'exploitation de l'ensemble des vulnérabilités corrigées 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 08 Novembre 2022**.**

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 08 Novembre 2022**:**

- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41128
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41091
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41073
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41125

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