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 dans Microsoft Windows (Patch Tuesday Juin 2022)
Numéro de Référence	36841506/22
Date de Publication	15 Juin 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- Windows Server 2022
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 21H2 pour x64-based Systems
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1
- Windows 10 Version 1809 pour ARM64-based Systems
- Windows 10 Version 1809 pour x64-based Systems
- Windows 10 Version 21H1 pour 32-bit Systems
- Windows 10 Version 21H2 pour ARM64-based Systems
- Windows 10 Version 21H2 pour 32-bit Systems
- Windows 11 pour ARM64-based Systems
- Windows 10 Version 20H2 pour ARM64-based Systems
- Windows 10 Version 20H2 pour 32-bit Systems
- Windows RT 8.1
- Windows 8.1 pour x64-based systems
- Windows 8.1 pour 32-bit systems
- Windows 10 Version 1809 pour 32-bit Systems
- Windows 7 pour x64-based Systems Service Pack 1
- Windows Server 2008 pour x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour x64-based Systems Service Pack 2
- Windows 7 pour 32-bit Systems 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 Server 2008 pour 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour 32-bit Systems Service Pack 2

Identificateurs externes

- CVE-2022-30190 CVE-2022-30151 CVE-2022-30142 CVE-2022-30193 CVE-2022-30150 CVE-2022-21123 CVE-2022-30148 CVE-2022-30147 CVE-2022-30140 CVE-2022-30131 CVE-2022-30167 CVE-2022-30141 CVE-2022-30139 CVE-2022-22018 CVE-2022-30136 CVE-2022-30135 CVE-2022-30132 CVE-2022-29119 CVE-2022-29111 CVE-2022-21125 CVE-2022-21166 CVE-2022-30189

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques y compris la critique faille « Follina » largement exploitée affectant les systèmes d'exploitation Windows sus-mentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant de divulguer des informations confidentielles, exécuter du code arbitraire, réussir une élévation de privilèges ou causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 14 Juin 2022**.**

Risque

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

Annexe

Bulletin de sécurité Microsoft du 14 Juin 2022 **:**

- https://msrc.microsoft.com/update-guide/