**ROYAUME DU MAROC**

**ADMINISTRATION**
**DE LA DEFENSE NATIONALE**

**Direction Générale de la Sécurité des Systèmes d'Information**

**Centre de Veille de Détection et de Réaction aux Attaques Informatiques**

**المملكة المغربية**

**إدارة الدفاع الوطني**

**المديرية العامة لأمن نظم المعلومات**

**مركز اليقظة والرصد والتصدي للهجمات المعلوماتية**

# BULLETIN DE SECURITE

| | |
|---|---|
| **Titre** | Vulnérabilités affectant Microsoft Windows (Patch Tuesday Septembre 2020) |
| **Numéro de Référence** | 26630909/20 |
| **Risque** | Important |
| **Impact** | Important |

## Systèmes affectés

- Windows Server, version 1903 (Server Core installation)
- Windows 10 Version 2004 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows Server 2019
- Windows 10 Version 2004 for ARM64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1803 for ARM64-based Systems
- Windows 10 Version 1803 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows Server, version 2004 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)
- Windows 10 Version 1803 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 2004 for x64-based Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1709 for 32-bit Systems
- Windows Server 2019 (Server Core installation)
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems

- Windows 10 Version 1709 for ARM64-based Systems
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows 10 Version 1709 for x64-based Systems
- Windows Server 2012
- Windows 8.1 for 32-bit systems
- Windows RT 8.1
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows Server 2012 (Server Core installation)
- Windows 10 Version 1607 for x64-based Systems
- Windows 8.1 for x64-based systems
- Windows Server, version 1803 (Server Core Installation)

## Identificateurs externes

CVE-2020-1507 CVE-2020-1590 CVE-2020-1471 CVE-2020-1532 CVE-2020-1592 CVE-2020-0790 CVE-2020-0718 CVE-2020-0648 CVE-2020-0837 CVE-2020-0664 CVE-2020-0914 CVE-2020-0839 CVE-2020-0951 CVE-2020-0922 CVE-2020-0941 CVE-2020-0928 CVE-2020-1013 CVE-2020-0805 CVE-2020-1034 CVE-2020-1038 CVE-2020-1039 CVE-2020-1146 CVE-2020-1122 CVE-2020-1169 CVE-2020-1130 CVE-2020-1285 CVE-2020-1376 CVE-2020-1508 CVE-2020-1491 CVE-2020-1596 CVE-2020-1559 CVE-2020-1589 CVE-2020-0766 CVE-2020-1593 CVE-2020-0782 CVE-2020-0890 CVE-2020-1598 CVE-2020-0761 CVE-2020-0908 CVE-2020-0911 CVE-2020-0838 CVE-2020-0912 CVE-2020-0856 CVE-2020-0921 CVE-2020-0875 CVE-2020-0989 CVE-2020-0904 CVE-2020-0886 CVE-2020-0998 CVE-2020-1030 CVE-2020-0836 CVE-2020-0870 CVE-2020-1031 CVE-2020-1052 CVE-2020-1053 CVE-2020-1074 CVE-2020-1033 CVE-2020-1091 CVE-2020-1097 CVE-2020-1083 CVE-2020-1129 CVE-2020-1115 CVE-2020-0997 CVE-2020-1250 CVE-2020-1119 CVE-2020-1098 CVE-2020-1252 CVE-2020-1133 CVE-2020-1152 CVE-2020-1308 CVE-2020-1303 CVE-2020-16854 CVE-2020-1159 CVE-2020-16879 CVE-2020-1245 CVE-2020-1319 CVE-2020-1228 CVE-2020-1256

## Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant son système d'exploitation Windows. Plusieurs de ces vulnérabilités sont critiques et leur exploitation peut permettre à un attaquant de provoquer une élévation de privilèges, divulguer des informations confidentielles, exécuter du code arbitraire à distance ou causer un déni de service.

## Solution

Veuillez-vous référer au guide de sécurité de Microsoft pour obtenir les nouvelles mises à jour.

## Risque

- Exécution de code arbitraire à distance.
- Déni de service.
- Accès à des informations confidentielles.
- Elévation de privilèges.

## Référence

Guide de sécurité de Microsoft :

- https://portal.msrc.microsoft.com/en-us/security-guidance