



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant Microsoft Windows (Patch Tuesday Janvier 2021)
<b>Numéro de Référence</b>	28351301/21
<b>Date de Publication</b>	13 Janvier 2021
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Remote Desktop client pour Windows Desktop
- Windows 10 Version 1607 pour systèmes 32 bits
- Windows 10 Version 1607 pour systèmes x64
- Windows 10 Version 1803 pour ARM64-based Systems
- Windows 10 Version 1803 pour systèmes 32 bits
- Windows 10 Version 1803 pour systèmes x64
- Windows 10 Version 1809 pour ARM64-based Systems
- Windows 10 Version 1809 pour systèmes 32 bits
- Windows 10 Version 1809 pour systèmes x64
- Windows 10 Version 1909 pour ARM64-based Systems
- Windows 10 Version 1909 pour systèmes 32 bits
- Windows 10 Version 1909 pour systèmes x64
- Windows 10 Version 2004 pour ARM64-based Systems
- Windows 10 Version 2004 pour systèmes 32 bits
- Windows 10 Version 2004 pour systèmes x64
- Windows 10 Version 20H2 pour ARM64-based Systems
- Windows 10 Version 20H2 pour systèmes 32 bits
- Windows 10 Version 20H2 pour systèmes x64
- Windows 10 pour systèmes 32 bits
- Windows 10 pour systèmes x64
- Windows 7 pour systèmes 32 bits Service Pack 1
- Windows 7 pour systèmes x64 Service Pack 1
- Windows 8.1 pour systèmes 32 bits
- Windows 8.1 pour systèmes x64
- Windows Defender

- 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, version 1909 (Server Core installation)
- Windows Server, version 2004 (Server Core installation)
- Windows Server, version 20H2 (Server Core Installation)

### Identificateurs externes

- CVE-2021-1708 CVE-2021-1648 CVE-2021-1650 CVE-2021-1649 CVE-2021-1652
- CVE-2021-1645 CVE-2021-1654 CVE-2021-1653 CVE-2021-1656 CVE-2021-1646
- CVE-2021-1659 CVE-2021-1662 CVE-2021-1660 CVE-2021-1664 CVE-2021-1666
- CVE-2021-1663 CVE-2021-1668 CVE-2021-1671 CVE-2021-1669 CVE-2021-1679
- CVE-2021-1678 CVE-2021-1680 CVE-2021-1685 CVE-2021-1688 CVE-2021-1691
- CVE-2021-1694 CVE-2021-1692 CVE-2021-1696 CVE-2021-1693 CVE-2021-1701
- CVE-2021-1702 CVE-2021-1697 CVE-2021-1704 CVE-2021-1700 CVE-2021-1710
- CVE-2021-1642 CVE-2021-1703 CVE-2021-1637 CVE-2021-1651 CVE-2021-1655
- CVE-2021-1638 CVE-2021-1657 CVE-2021-1658 CVE-2021-1665 CVE-2021-1661
- CVE-2021-1667 CVE-2021-1673 CVE-2021-1672 CVE-2021-1676 CVE-2021-1674
- CVE-2021-1670 CVE-2021-1682 CVE-2021-1684 CVE-2021-1683 CVE-2021-1690
- CVE-2021-1687 CVE-2021-1681 CVE-2021-1695 CVE-2021-1689 CVE-2021-1699
- CVE-2021-1709 CVE-2021-1706 CVE-2021-1686 CVE-2021-1647

### Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant ses systèmes d'exploitation Windows. L'exploitation de ces vulnérabilités peut permettre à un attaquant de divulguer des informations confidentielles, d'exécuter du code arbitraire, de réussir une élévation de privilèges ou de causer un déni de service.

## **Solution**

Veillez vous référer au bulletin de sécurité Microsoft du 12 Janvier 2021.

## **Risque**

- Divulgence d'informations ;
- Dénier de service ;
- Exécution de code à distance ;
- élévation de privilèges,

## **Annexe**

Bulletin de sécurité Microsoft du 12 Janvier 2021:

- <https://msrc.microsoft.com/update-guide/fr-FR>