



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité critique activement exploitée affectant les produits Microsoft
<b>Numéro de Référence</b>	63662904/26
<b>Date de Publication</b>	29 Avril 2026
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- .NET 10.0 installé sur Linux
- .NET 10.0 installé sur Mac OS
- .NET 10.0 installé sur Windows
- .NET 8.0 installé sur Linux
- .NET 8.0 installé sur Mac OS
- .NET 8.0 installé sur Windows
- .NET 9.0 installé sur Linux
- .NET 9.0 installé sur Mac OS
- .NET 9.0 installé sur Windows
- Azure Logic Apps
- Azure Monitor Agent
- Microsoft .NET Framework
- Microsoft .NET Framework 3.5 AND 4.8.1
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
- Microsoft 365 Apps pour Enterprise
- Microsoft Defender Antimalware Platform
- Microsoft Dynamics 365
- Microsoft Excel 2016
- Microsoft HPC Pack 2019
- Microsoft Office 2016

- Microsoft Office 2019
- Microsoft Office LTSC 2021
- Microsoft Office LTSC 2024
- Microsoft Office LTSC pour Mac 2021
- Microsoft Office LTSC pour Mac 2024
- Microsoft Power Apps
- Microsoft PowerPoint 2016
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft SQL Server 2022
- Microsoft SQL Server 2025
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Visual Studio 2022
- Microsoft Visual Studio Code CoPilot Chat Extension
- Office Online Server
- PowerShell
- Remote Desktop client pour Windows Desktop
- Windows 10
- Windows 11
- Windows Admin Center
- Windows App Client pour Windows Desktop
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 202

### **Identificateurs externes**

- CVE-2026-32201;

### **Bilan de la vulnérabilité**

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 البقطة 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

La vulnérabilité affectant les produits Microsoft susmentionnés, identifiée par «CVE-2026-32201» et qui a fait l'objet du bulletin «63131504/26» de la DGSSI est activement exploitée. Cette vulnérabilité peut permettre à un attaquant de réussir une usurpation d'identité et accéder à des informations confidentielles par la suite.

## **Solution**

Veillez se référer au bulletin de sécurité Microsoft pour plus d'information.

## **Risque**

- Usurpation d'identité ;

## **Annexe**

Bulletin de sécurité Microsoft du 28 Avril 2026:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32202>
- <https://www.dgssi.gov.ma/fr/bulletins/vulnerabilites-dans-microsoft-windows-patch-tuesday-avril-2026/>