



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans Microsoft Office (Patch Tuesday Mai 2024)
<b>Numéro de Référence</b>	47431505/24
<b>Date de Publication</b>	15 Mai 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systèmes affectés

- Microsoft 365 Apps pour Enterprise pour 64-bit Systems
- Microsoft 365 Apps pour Enterprise pour 32-bit Systems
- Microsoft Office 2019 pour 64-bit editions
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 64-bit editions
- Microsoft Office LTSC pour Mac 2021
- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Office 2019 pour 32-bit editions
- Office Online Server

### Identificateurs externes

- CVE-2024-30042 CVE-2024-30044 CVE-2024-30043

### Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques, y compris un zero-day « CVE-2024-30044 » activement exploité, affectant Microsoft SharePoint permettant la divulgation des informations confidentielles. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données.

## **Solution**

Veillez se référer au bulletin de sécurité Microsoft du 14 Mai 2024.

## **Risque**

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données

## **Annexe**

Bulletin de sécurité Microsoft du 14 Mai 2024:

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