



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans Microsoft Office (Patch Tuesday Mai 2025)
<b>Numéro de Référence</b>	54441405/25
<b>Date de Publication</b>	14 Mai 2025
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Microsoft 365 Apps for Enterprise pour les systèmes 32 bits
- Microsoft Office 2019 pour les éditions 32 bits
- Microsoft Excel 2016 (édition 64 bits)
- Microsoft Excel 2016 (édition 32 bits)
- Microsoft Office LTSC 2024 pour les éditions 64 bits
- Microsoft Office LTSC 2024 pour les éditions 32 bits
- Microsoft Office LTSC 2021 pour les éditions 32 bits
- Microsoft Office LTSC 2021 pour les éditions 64 bits
- Microsoft 365 Apps for Enterprise pour les systèmes 64 bits
- Microsoft Office 2019 pour les éditions 64 bits
- Microsoft Office LTSC pour Mac 2024
- Microsoft Office pour Universal
- Microsoft Office pour Android
- Microsoft Office LTSC pour Mac 2021
- Microsoft Office 2016 (édition 64 bits)
- Microsoft Office 2016 (édition 32 bits)
- Microsoft SharePoint Server Edition d'abonnement
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016
- Office Online Server

## Identificateurs externes

- CVE-2025-30393 CVE-2025-30377 CVE-2025-30376
- CVE-2025-32705 CVE-2025-32704 CVE-2025-30388
- CVE-2025-30386 CVE-2025-30384 CVE-2025-30383
- CVE-2025-30382 CVE-2025-30381 CVE-2025-30379
- CVE-2025-30378 CVE-2025-30375 CVE-2025-29979
- CVE-2025-29978 CVE-2025-29977 CVE-2025-29976

## Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft office. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code arbitraire à distance et de réussir une élévation de privilèges.

## Solution

Veillez se référer au bulletin de sécurité Microsoft du 13 Mai 2025.

## Risque

- Exécution du code arbitraire à distance
- Elévation de privilèges

## Annexe

Bulletin de sécurité Microsoft du 13 Mai 2025:

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