



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Microsoft Office (Patch Tuesday Avril 2025)
Numéro de Référence	53790904/25
Date de Publication	09 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft 365 Apps pour Enterprise pour 32-bit Systems
- Microsoft 365 Apps pour Enterprise pour 64-bit Systems
- Microsoft Access 2016 (32-bit edition)
- Microsoft Access 2016 (64-bit edition)
- Microsoft AutoUpdate pour Mac
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2019 pour 32-bit editions
- Microsoft Office 2019 pour 64-bit editions
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 64-bit editions
- Microsoft Office LTSC 2024 pour 32-bit editions
- Microsoft Office LTSC 2024 pour 64-bit editions
- Microsoft Office LTSC pour Mac 2021
- Microsoft Office LTSC pour Mac 2024
- Microsoft Office pour Android
- Microsoft Office pour Universal
- Microsoft OneNote 2016 (32-bit edition)

- Microsoft OneNote 2016 (64-bit edition)
- Microsoft OneNote pour Mac
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Office Online Server
- SharePoint Server Subscription Edition Language Pack

Identificateurs externes

- CVE-2025-29801 CVE-2025-29800 CVE-2025-26642
- CVE-2025-29816 CVE-2025-29823 CVE-2025-29822
- CVE-2025-29820 CVE-2025-29794 CVE-2025-29792
- CVE-2025-29793 CVE-2025-29791 CVE-2025-27750
- CVE-2025-27752 CVE-2025-27751 CVE-2025-27749
- CVE-2025-27747 CVE-2025-27748 CVE-2025-27746
- CVE-2025-27745 CVE-2025-27744 CVE-2025-26687

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, de réussir une élévation de privilèges ou de contourner la politique de sécurité.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 08 Avril 2025.

Risque

- Exécution du code arbitraire à distance
- Contournement de la politique de sécurité
- Elévation de privilèges

Annexe

Bulletin de sécurité Microsoft du 08 Avril 2025:

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