



BULLETIN DE SECURITE

Titre	Vulnérabilités dans Microsoft Office (Patch Tuesday Février 2026)
Numéro de Référence	60921102/26
Date de Publication	10 Février 2026
Risque	Important
Impact	Important

Systèmes affectés

- Microsoft Office LTSC pour Mac 2021
- 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 Office 2019 pour 32-bit editions
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Office LTSC pour Mac 2024
- Microsoft Office LTSC 2024 pour 64-bit editions
- Microsoft Office LTSC 2024 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 64-bit editions
- Office Online Server
- Microsoft Word 2016 (64-bit edition)
- Microsoft Word 2016 (32-bit edition)
- Microsoft SharePoint Server Subscription Edition
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft Outlook 2016 (32-bit edition)

Identificateurs externes

- CVE-2026-21511 CVE-2026-21261 CVE-2026-21514 CVE-2026-21260
- CVE-2026-21258 CVE-2026-21259 ;

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 de réussir une élévation de privilèges, de divulguer des informations confidentielles et de contourner la politique de sécurité.

Solution

Veillez se référer au bulletin de sécurité Microsoft du 10 Février 2026.

Risque

- Contournement de la politique de sécurité ;
- Elévation de privilèges ;
- Divulcation des informations confidentielles ;

Annexe

Bulletin de sécurité Microsoft du 10 Février 2026:

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