ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Microsoft Office (Patch Tuesday Février 2024)
Numéro de Référence	46001402/24
Date de Publication	14 Février 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Word 2016 (64-bit edition)
- Microsoft Word 2016 (32-bit edition)
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC 2021 pour 64-bit editions
- 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 Outlook 2016 (64-bit edition)
- Microsoft Outlook 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Visio 2016 (64-bit edition)
- Microsoft Visio 2016 (32-bit edition)
- Microsoft PowerPoint 2016 (64-bit edition)
- Microsoft PowerPoint 2016 (32-bit edition)
- Skype pour Business 2016 (64-bit)
- Skype pour Business 2016 (32-bit)

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 اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Microsoft Publisher 2016 (64-bit edition)
- Microsoft Publisher 2016 (32-bit edition)
- Microsoft Teams pour Android
- Skype pour Business Server 2019 CU7

Identificateurs externes

- CVE-2024-21379 CVE-2024-21413 CVE-2024-21402 CVE-2024-21378 CVE-2024-20673 CVE-2024-21384 CVE-2024-21374 CVE-2024-20695

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées des 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 et de divulguer des informations confidentielles.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 13 Février 2024**.**

Risque

- Exécution du code arbitraire à distance
- Elévation de privilège
- Divulgation d'information confidentielle

Annexe

Bulletin de sécurité Microsoft du 13 Février 2024**:**

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

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 اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma