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 2023)
Numéro de Référence	40271502/23
Date de Publication	15 Février 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft OneNote pour Android
- Microsoft Office pour iOS
- Microsoft Office pour Universal
- Microsoft Office pour Android
- Microsoft 365 Apps pour Enterprise pour 32-bit Systems
- Microsoft 365 Apps pour Enterprise pour 64-bit Systems
- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft Office Web Apps Server 2013 Service Pack 1
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft Office 2019 pour Mac
- Microsoft Office Online Server
- SharePoint Server Subscription Edition Language Pack
- Microsoft Office LTSC 2021 pour 64-bit editions

- Microsoft SharePoint Server Subscription Edition
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office LTSC pour Mac 2021

Identificateurs externes

- CVE-2023-21721 CVE-2023-21823 CVE-2023-21715 CVE-2023-21716 CVE-2023-21717 CVE-2023-21714

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les versions susmentionnées des produits Microsoft Office. Selon Microsoft, une de ces vulnérabilités identifiée par «CVE-2023-21715» est un « Zero-day » et peut permettre à un attaquant d'exécuter du code arbitraire. L'exploitation de ces vulnérabilités peut permettre à un attaquant de réussir une élévation de privilèges, d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité de données, de réussir une usurpation d'identité et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 14 Février 2023**.**

Risque

- Elévation de privilèges
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité de données
- Usurpation d'identité
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Microsoft du 14 Février 2023**:**

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