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 Septembre 2023)
Numéro de Référence	43681309/23
Date de Publication	13 Septembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Office 2019 pour 32-bit editions
- Microsoft Office 2019 pour 64-bit editions
- Microsoft Office 2019 pour Mac
- Microsoft 365 Apps pour Enterprise pour 32-bit Systems
- Microsoft 365 Apps pour Enterprise pour 64-bit Systems
- Microsoft Office LTSC pour Mac 2021
- Microsoft Office LTSC 2021 pour 64-bit editions
- Microsoft Office LTSC 2021 pour 32-bit editions
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2013 RT Service Pack 1
- Microsoft Office 2013 Service Pack 1 (32-bit editions)
- Microsoft Office 2013 Service Pack 1 (64-bit editions)
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server Subscription Edition
- Microsoft Outlook 2016 (32-bit edition)
- Microsoft Outlook 2016 (64-bit edition)
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)

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 Office Online Server
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)
- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2013 RT Service Pack 1
- Microsoft Excel 2013 Service Pack 1 (32-bit editions)
- Microsoft Excel 2013 Service Pack 1 (64-bit editions)

Identificateurs externes

- CVE-2023-36767 CVE-2023-36765 CVE-2023-36764 CVE-2023-36763 CVE-2023-36762 CVE-2023-36761 CVE-2023-36766 CVE-2023-41764

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-2023-36767» activement exploitée peut être utilisée pour voler les hashs NTLM lors de l'ouverture d'un document. Ces hashs NTLM peuvent être craqués ou utilisés dans des attaques « NTLM Relay » pour obtenir l'accès au compte.

Par conséquent, l'exploitation du reste des vulnérabilités pourrait 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 12 Septembre 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 12 Septembre 2023**:**

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