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 Mars 2023)
Numéro de Référence	40821503/23
Date de Publication	15 Mars 2023
Risque	Critique
Impact	Critique

Systèmes affectés

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

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 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Excel 2016 (64-bit edition)
- Microsoft Excel 2016 (32-bit edition)
- Microsoft Office Online Server
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Windows Server 2008 R2 pour x64-based Systems Service Pack 1
- Windows Server 2008 pour x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour x64-based Systems Service Pack 2
- Windows Server 2008 pour 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 pour 32-bit Systems Service Pack 2

Identificateurs externes

- CVE-2023-24930 , CVE-2023-24882 , CVE-2023-24923 , CVE-2023-24910 , CVE-2023-23391 , CVE-2023-23397 , CVE-2023-23399 , CVE-2023-23398 , CVE-2023-23396 , CVE-2023-23395

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-2023-23397» affectant Microsoft Outlook est activement exploitée et peut permettre à un attaquant de réussir une élévation de privilèges.

Microsoft ajoute qu'un attaquant pourrait exploiter cette faille en envoyant un courriel spécialement conçu au client Outlook de Windows. Cela pourrait conduire à une exploitation sans nécessiter d'interaction de la part de l'utilisateur et avant même que le message ne soit visualisé.

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 14 Mars 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 Mars 2023**:**

- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

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