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 plusieurs produits Microsoft (Patch Tuesday Février 2023)
Numéro de Référence	40311502/23
Date de Publication	15 Février 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Visual Studio 2022 version 17.4
- Microsoft Visual Studio 2022 version 17.0
- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
- Microsoft Visual Studio 2022 version 17.2
- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
- Microsoft .NET Framework 3.5 AND 4.7.2
- Microsoft .NET Framework 3.5 AND 4.8
- Microsoft .NET Framework 3.5 AND 4.8.1
- Microsoft .NET Framework 4.8
- Microsoft .NET Framework 3.5 and 4.6.2
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft Defender Security Intelligence Updates
- Power BI Report Server - January 2023
- HoloLens 1
- Microsoft Dynamics 365 Unified Service Desk

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

- 3D Builder
- Print 3D
- Microsoft Defender pour IoT
- Microsoft Dynamics 365 (on-premises) version 9.0
- Microsoft Dynamics 365 (on-premises) version 9.1
- Microsoft SQL Server 2017 pour x64-based Systems (GDR)
- Microsoft SQL Server 2016 pour x64-based Systems Service Pack 3 (GDR)
- Microsoft SQL Server 2022 pour x64-based Systems (GDR)
- Microsoft SQL Server 2019 pour x64-based Systems (CU 18)
- Microsoft SQL Server 2016 pour x64-based Systems Service Pack 3 Azure Connectivity Pack
- Microsoft SQL Server 2014 Service Pack 3 pour 32-bit Systems (GDR)
- Microsoft SQL Server 2019 pour x64-based Systems (GDR)
- Microsoft SQL Server 2014 Service Pack 3 pour x64-based Systems (GDR)
- Microsoft SQL Server 2014 Service Pack 3 pour x64-based Systems (CU 4)
- Microsoft SQL Server 2017 pour x64-based Systems (CU 31)
- Microsoft SQL Server 2014 Service Pack 3 pour 32-bit Systems (CU 4)
- .NET 6.0
- .NET 7.0

Identificateurs externes

- CVE-2023-41953 CVE-2022-23521 CVE-2023-21722 CVE-2023-21808 CVE-2023-21823 CVE-2023-21809 CVE-2023-21806 CVE-2019-15126 CVE-2023-21778 CVE-2023-23390 CVE-2023-23378 CVE-2023-21815 CVE-2023-23381 CVE-2023-23379 CVE-2023-23377 CVE-2023-21573 CVE-2023-21572 CVE-2023-21571 CVE-2023-23376 CVE-2023-21570 CVE-2023-21568 CVE-2023-21713 CVE-2023-21718 CVE-2023-21528 CVE-2023-21704 CVE-2023-21705 CVE-2023-21567 CVE-2023-21566 CVE-2023-21807 CVE-2023-21553 CVE-2023-21805 CVE-2023-21702 CVE-2023-21701 CVE-2023-21700 CVE-2023-21699 CVE-2023-21697 CVE-2023-21695 CVE-2023-21694 CVE-2023-21693 CVE-2023-21692 CVE-2023-21691 CVE-2023-21690 CVE-2023-21689 CVE-2023-21688 CVE-2023-21686 CVE-2023-21685 CVE-2023-21822 CVE-2023-21820 CVE-2023-21818 CVE-2023-21817 CVE-2023-21816 CVE-2023-21813 CVE-2023-21812 CVE-2023-21811 CVE-2023-21803 CVE-2023-21802 CVE-2023-21801 CVE-2023-21800 CVE-2023-21799 CVE-2023-21798 CVE-2023-21797 CVE-2023-21684 CVE-2023-23374 CVE-2023-21794 CVE-2023-21720

Bilan de la vulnérabilité

Microsoft annonce la correction de plusieurs vulnérabilités critiques affectant les produits Microsoft susmentionnés. 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 at-

teinte 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/fr-FR