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 Avril 2024)
Numéro de Référence	47001504/24
Date de Publication	15 Avril 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft Visual Studio 2022 version 17.9 versions antérieures à 17.9.6
- Microsoft Visual Studio 2022 version 17.8 versions antérieures à 17.8.9
- Microsoft Visual Studio 2022 version 17.6 versions antérieures à 17.6.14
- Microsoft Visual Studio 2022 version 17.4 versions antérieures à 17.4.18
- Microsoft Visual Studio 2019 version 16.11 (inclut les versions 16.0 à 16.10) versions antérieures à 16.11.35
- Microsoft SharePoint Server Subscription Edition versions antérieures à 16.0.17328.20246
- Microsoft SharePoint Server 2019 versions antérieures à 16.0.10409.20027
- Microsoft SharePoint Server 2016 versions antérieures à 16.0.5443.1000
- Microsoft SQL Server 2022 pour systèmes x64 (GDR) versions antérieures à 16.0.1115.1
- Microsoft SQL Server 2022 pour systèmes x64 (CU 12) versions antérieures à 16.0.4120.1
- Microsoft SQL Server 2019 pour systèmes x64 (GDR) versions antérieures à 15.0.2110.4
- Microsoft SQL Server 2019 pour systèmes x64 (CU 25) versions antérieures à 15.0.4360.2
- Microsoft OLE DB Driver 19 pour SQL Server versions antérieures à 19.3.0003.0
- Microsoft OLE DB Driver 18 pour SQL Server versions antérieures à 18.7.0002.0
- Microsoft ODBC Driver 18 pour SQL Server sur MacOS versions antérieures à 18.3.3.1

- Microsoft ODBC Driver 18 pour SQL Server sur Linux versions antérieures à 18.3.3.1
- Microsoft ODBC Driver 17 pour SQL Server sur MacOS versions antérieures à 17.10.6.1
- Microsoft ODBC Driver 17 pour SQL Server sur Linux versions antérieures à 17.10.6.1
- Microsoft Defender pour IoT versions antérieures à 24.1.3
- Microsoft .NET Framework 4.8 versions antérieures à 4.8.4718.0
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 versions antérieures à 4.7.4092.0
- Microsoft .NET Framework 4.6.2 versions antérieures à 4.7.4092.0
- Microsoft .NET Framework 3.5 AND 4.8.1 versions antérieures à 4.8.9236.0
- Microsoft .NET Framework 3.5 AND 4.8.1 versions antérieures à 4.8.9206.0
- Microsoft .NET Framework 3.5 AND 4.8 versions antérieures à 4.8.4718.0
- Microsoft .NET Framework 3.5 AND 4.7.2 versions antérieures à 4.7.4092.0
- Microsoft .NET Framework 3.5 AND 4.7.2 versions antérieures à 10.0.14393.6897
- .NET 8.0 versions antérieures à 8.0.4
- .NET 7.0 versions antérieures à 7.0.18
- .NET 6.0 versions antérieures à 6.0.29

Identificateurs externes

- CVE-2024-21409 CVE-2024-29985 CVE-2024-29984 CVE-2024-29983 CVE-2024-29982 CVE-2024-29055 CVE-2024-29054 CVE-2024-29053 CVE-2024-29048 CVE-2024-29047 CVE-2024-29046 CVE-2024-29045 CVE-2024-29044 CVE-2024-29043 CVE-2024-28945 CVE-2024-28944 CVE-2024-28943 CVE-2024-28942 CVE-2024-28941 CVE-2024-28940 CVE-2024-28939 CVE-2024-28938 CVE-2024-28937 CVE-2024-28936 CVE-2024-28935 CVE-2024-28934 CVE-2024-28933 CVE-2024-28932 CVE-2024-28931 CVE-2024-28930 CVE-2024-28929 CVE-2024-28927 CVE-2024-28926 CVE-2024-28915 CVE-2024-28914 CVE-2024-28913 CVE-2024-28912 CVE-2024-28911 CVE-2024-28910 CVE-2024-28909 CVE-2024-28908 CVE-2024-28906 CVE-2024-26251 CVE-2024-21409 CVE-2024-21324 CVE-2024-21323 CVE-2024-21322

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 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 09 avril 2024**.**

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

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 09 avril 2024**:**

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

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma