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 Novembre 2023)
Numéro de Référence	44781511/23
Date de Publication	15 Novembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft .NET Framework 3.5 AND 4.7.2
- Microsoft .NET Framework 3.5 AND 4.8
- Microsoft .NET Framework 4.8
- 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 .NET Framework 3.5 AND 4.6/4.6.2
- Microsoft .NET Framework 4.6.2
- Microsoft .NET Framework 3.5 AND 4.8.1
- Microsoft Dynamics 365 (on-premises) version 9.1
- Microsoft Visual Studio 2022 version 17.4
- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
- Microsoft Visual Studio 2022 version 17.2
- Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
- Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
- Microsoft Dynamics 365 (on-premises) version 9.0
- .NET 7.0
- .NET 6.0
- ASP.NET Core 8.0

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

- ASP.NET Core 7.0
- Microsoft Visual Studio 2022 version 17.7
- Microsoft Visual Studio 2022 version 17.6
- Send Customer Voice survey from Dynamics 365 app
- .NET 8.0
- Jupyter Extension pour Visual Studio Code
- System Center Operations Manager (SCOM) 2016
- System Center Operations Manager (SCOM) 2019
- System Center Operations Manager (SCOM) 2022
- Windows Defender Antimalware Platform
- ASP.NET Core 6.0

Identificateurs externes

- CVE-2023-36007 CVE-2023-36705 CVE-2023-36402 CVE-2023-36397 CVE-2023-36038 CVE-2023-36016 CVE-2023-36018 CVE-2023-36017 CVE-2023-36043 CVE-2023-36410 CVE-2023-36036 CVE-2023-36398 CVE-2023-36422

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 14 Novembre 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 Novembre 2023**:**

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