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 2023)
Numéro de Référence	41331204/23
Date de Publication	12 Avril 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Send Customer Voice survey from Dynamics 365
- Visual Studio Code
- Microsoft Dynamics 365 (on-premises) version 9.1
- Microsoft Dynamics 365 (on-premises) version 9.0
- Microsoft Visual Studio 2022 version 17.5
- Microsoft Visual Studio 2022 version 17.0
- Microsoft Visual Studio 2022 version 17.2
- Microsoft Visual Studio 2022 version 17.4
- Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
- Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
- .NET 7.0
- .NET 6.0
- Microsoft Malware Protection Engine

Identificateurs externes

- CVE-2023-21729 , CVE-2023-28313 , CVE-2023-24893 , CVE-2023-28314 , CVE-2023-28299 , CVE-2023-28296 , CVE-2023-28263 , CVE-2023-28262 , CVE-2023-28260 , CVE-2023-28309 , CVE-2023-28308 , CVE-2023-28307 , CVE-2023-28306 , CVE-2023-28305 , CVE-2023-28302 , CVE-2023-28298 , CVE-2023-28293 , CVE-2023-28256 , CVE-2023-28278 , CVE-2023-28255 , CVE-2023-28253 , CVE-2023-28254 , CVE-2023-28276 , CVE-2023-28275 , CVE-2023-28252 , CVE-2023-28250 , CVE-2023-28272 , CVE-2023-28271 , CVE-2023-28268 , CVE-2023-28244 , CVE-2023-28266 , CVE-2023-28267 , CVE-2023-28241 , CVE-2023-28240 , CVE-2023-

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

28238 , CVE-2023-28232 , CVE-2023-28231 , CVE-2023-28228 , CVE-2023-28229 , CVE-2023-28227 , CVE-2023-28223 , CVE-2023-28222 , CVE-2023-28220 , CVE-2023-28219 , CVE-2023-28218 , CVE-2023-28217 , CVE-2023-28216 , CVE-2023-24931 , CVE-2023-24912 , CVE-2023-24860 , CVE-2023-23384 , CVE-2023-21769 , CVE-2023-21727 , CVE-2023-21554

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 12 Avril 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 Avril 2023**:**

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