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 dans les produits Microsoft Azure (Patch Tuesday Juillet 2024)
Numéro de Référence	48191007/24
Date de Publication	10 Juillet 2024
Risque	Important
Impact	Important

Systèmes affectés

- Azure CycleCloud 8.5.0
- Azure CycleCloud 8.4.2
- Azure CycleCloud 8.4.0
- Azure CycleCloud 8.4.1
- Azure DevOps Server 2022.1
- Azure Network Watcher VM Extension pour Windows
- Azure CycleCloud 8.3.0
- Azure CycleCloud 8.2.2
- Azure CycleCloud 8.1.0
- Azure CycleCloud 8.2.1
- Azure CycleCloud 8.1.1
- Azure CycleCloud 8.0.2
- Azure CycleCloud 7.9.7
- Azure CycleCloud 7.9.5
- Azure CycleCloud 7.9.4
- Azure CycleCloud 7.9.6
- Azure CycleCloud 7.9.2
- Azure CycleCloud 8.0.1
- Azure CycleCloud 7.9.11
- Azure CycleCloud 7.9.8
- Azure CycleCloud 7.9.9
- Azure CycleCloud 7.9.1
- Azure CycleCloud 7.9.3
- Azure CycleCloud 7.9.0
- Azure CycleCloud 8.6.0
- Azure CycleCloud 8.0.0

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

- Azure CycleCloud 8.2.0
- Azure CycleCloud 7.9.10
- Azure Kinect SDK

Identificateurs externes

- CVE-2024-38092 CVE-2024-35267 CVE-2024-35266 CVE-2024-35261 CVE-2024-38086

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Azure susmentionnés. L'exploitation de ces failles permet à un attaquant de réussir une élévation de privilèges, d'exécuter du code arbitraire à distance ou de réussir une usurpation d'identité.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 09 Juillet 2024**.**

Risque

- Elévation de privilèges
- Exécution du code arbitraire à distance
- Usurpation d'identité

Annexe

Bulletin de sécurité Microsoft du 09 Juillet 2024**:**

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