ROYAUME DU MAROC ADMINISTRATION DE LA DEFENSE NATIONALE



المملكة المغربية إدارة الدفاع الوطني المديرية العامة لأمن نظم المعلومات

Direction Générale de la Sécurité des Systèmes d'Information

BULLETIN DE SECURITE

Titre	Vulnérabilités dans Microsoft Azure (Patch Tuesday Novembre 2024)
Numéro de Référence	50781311/24
Date de Publication	13 Novembre 2024
Risque	Important
Impact	Important

Systèmes affectés

- Azure Database pour PostgreSQL Flexible Server 12
- Azure Database pour PostgreSQL Flexible Server 13
- Azure Database pour PostgreSQL Flexible Server 14
- Azure Database pour PostgreSQL Flexible Server 15
- Azure Database pour PostgreSQL Flexible Server 16
- Azure CycleCloud 8.3.0
- Azure CycleCloud 8.5.0
- Azure CycleCloud 8.4.0
- Azure CycleCloud 8.4.2
- Azure CycleCloud 8.1.1
- Azure CycleCloud 8.4.1
- Azure CycleCloud 8.2.2
- Azure CycleCloud 8.2.1
- Azure CycleCloud 8.2.0
- Azure CycleCloud 8.1.0
- Azure CycleCloud 8.0.2
- Azure CycleCloud 8.6.1Azure CycleCloud 8.6.2
- Azure CycleCloud 8.6.0
- Azure CycleCloud 8.0.1
- Azure CycleCloud 8.0.0
- Azure CycleCloud 8.6.4
- Azure CycleCloud 8.6.3
- Azure Linux 3.0 ARM
- Azure Linux 3.0 x64

Identificateurs externes

• CVE-2024-43613 CVE-2024-49042 CVE-2024-49056 CVE-2024-43602

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 37 37 37 05 05 05 contact@macert.gov.ma البريد الإلكتروني

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 et d'exécuter du code arbitraire à distance.

Solution

Veuillez se référer au bulletin de sécurité Microsoft du 12 Novembre 2024.

Risque

- Elévation de privilèges
- Exécution du code arbitraire à distance

Annexe

Bulletin de sécurité Microsoft du 12 Novembre 2024:

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

B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53

Email: contact@macert.gov.ma