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 les produits Microsoft SQL Server (Patch Tuesday Novembre 2024)
Numéro de Référence	50771311/24
Date de Publication	13 Novembre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Microsoft SQL Server 2017 pour x64-based Systems (CU 31)
- Microsoft SQL Server 2016 pour x64-based Systems Service Pack 3 Azure Connect Feature Pack
- Microsoft SQL Server 2016 pour x64-based Systems Service Pack 3 (GDR)
- Microsoft SQL Server 2017 pour x64-based Systems (GDR)
- Microsoft SQL Server 2019 pour x64-based Systems (GDR)
- Microsoft SQL Server 2019 pour x64-based Systems (CU 29)
- Microsoft SQL Server 2022 pour x64-based Systems (CU 15)
- Microsoft SQL Server 2022 pour x64-based Systems (GDR)

Identificateurs externes

- CVE-2024-49012 CVE-2024-48993 CVE-2024-48996 CVE-2024-48995
- CVE-2024-49021 CVE-2024-49018 CVE-2024-49017 CVE-2024-49016
- CVE-2024-49015 CVE-2024-49014 CVE-2024-49013 CVE-2024-49011
- CVE-2024-49010 CVE-2024-49009 CVE-2024-49008 CVE-2024-49006
- CVE-2024-49007 CVE-2024-49005 CVE-2024-49004 CVE-2024-49003

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

- CVE-2024-49002 CVE-2024-49001 CVE-2024-49000 CVE-2024-48999
- CVE-2024-48998 CVE-2024-48997 CVE-2024-49043 CVE-2024-48994
- CVE-2024-43462 CVE-2024-43459 CVE-2024-38255

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les versions de Microsoft SQL Server susmentionnées. L'exploitation de ces failles permet à un attaquant d'exécuter du code arbitraire à distance et de contourner la politique de sécurité.

Solution

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

Risque

- Exécution du code arbitraire à distance
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Microsoft du 12 Novembre 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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma