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 IBM
Numéro de Référence	53730704/25
Date de Publication	07 Avril 2025
Risque	Important
Impact	Important

Systèmes affectés

- QRadar Analyst Workflow versions antérieures à 3.0.0
- WebSphere Application Server Liberty version 17.0.0.3 à 25.0.0.3
- WebSphere Hybrid Edition version 5.1
- Db2 versions antérieures à 5.1.2 pour Cloud Pak for Data
- Db2 Warehouse versions antérieures à 5.1.2 pour Cloud Pak for Data

Identificateurs externes

- CVE-2018-20225 CVE-2018-6341 CVE-2019-11253
- CVE-2020-13844 CVE-2021-23337 CVE-2021-4204
- CVE-2021-44906 CVE-2021-47495 CVE-2022-29153
- CVE-2022-48706 CVE-2022-48890 CVE-2022-48921
- CVE-2023-43804 CVE-2023-44487 CVE-2023-45142
- CVE-2023-45857 CVE-2023-52455 CVE-2023-52467
- CVE-2023-52605 CVE-2023-52832 CVE-2023-52885
- CVE-2023-52898 CVE-2024-26740 CVE-2024-26776
- CVE-2024-26843 CVE-2024-27281 CVE-2024-34997
- CVE-2024-35176 CVE-2024-35790 CVE-2024-35946
- CVE-2024-36620 CVE-2024-37071 CVE-2024-39494
- CVE-2024-39908 CVE-2024-40679 CVE-2024-41110
- CVE-2024-41123 CVE-2024-41761 CVE-2024-41762
- CVE-2024-41946 CVE-2024-43398 CVE-2024-45296
- CVE-2024-45337 CVE-2024-45338 CVE-2024-45663
- CVE-2024-47764 CVE-2024-49761 CVE-2024-51479
- CVE-2024-52798 CVE-2024-6119 CVE-2024-6232

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-2024-6484 CVE-2024-6485 CVE-2025-23184
- CVE-2025-25285 CVE-2025-25288 CVE-2025-25289
- CVE-2025-25290 CVE-2025-27152

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits IBM susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, de contourner la politique de sécurité, de porter atteinte à la confidentialité des données, d'injecter du code indirecte à distance (XSS), une élévation de privilèges ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité IBM pour plus d'information.

Risque

- Atteinte à la confidentialité des données
- Injection de code indirecte à distance (XSS)
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance
- Déni de service
- Elévation de privilèges

Annexe

Bulletin de sécurité IBM:

- https://www.ibm.com/support/pages/node/7229443
- https://www.ibm.com/support/pages/node/7229768
- https://www.ibm.com/support/pages/node/7229770
- https://www.ibm.com/support/pages/node/7229772
- https://www.ibm.com/support/pages/node/7230024