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	61720603/26
Date de Publication	06 Mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- DB2 Data Management Console versions antérieures à 3.1.13 ;
- Db2 on Cloud Pak for Data versions antérieures à 5.3.1 ;
- DB2 Recovery Expert versions antérieures à 5.5.0.1 Interim Fix 8 ;
- Db2 Warehouse on Cloud Pak for Data versions antérieures à 5.3.1 ;
- QRadar Data Synchronization App versions antérieures à 3.3.0 ;
- QRadar Pre-Validation App versions antérieures à 2.0.2 ;
- Tivoli Netcool/OMNIbus_GUI ;

Identificateurs externes

- CVE-2012-2098, CVE-2015-1283, CVE-2015-2716, CVE-2016-0703, CVE-2016-0704
- CVE-2016-0800, CVE-2016-4472, CVE-2016-4658, CVE-2016-9318, CVE-2018-14040
- CVE-2018-14041, CVE-2018-14042, CVE-2018-5764, CVE-2019-19921, CVE-2019-8331
- CVE-2020-15115, CVE-2021-20251, CVE-2021-22569, CVE-2021-22570, CVE-2021-33036
- CVE-2021-37404, CVE-2022-21426, CVE-2022-21619, CVE-2022-21624, CVE-2022-21626
- CVE-2022-21628, CVE-2022-29154, CVE-2022-29458, CVE-2022-3171, CVE-2022-32743
- CVE-2022-3509, CVE-2022-3510, CVE-2022-40609, CVE-2022-40897, CVE-2022-4304
- CVE-2022-4450, CVE-2022-45047, CVE-2022-46337, CVE-2023-0215, CVE-2023-0286
- CVE-2023-21830, CVE-2023-21843, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938
- CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2023-22041
- CVE-2023-22043, CVE-2023-22044, CVE-2023-22045, CVE-2023-22049, CVE-2023-22067
- CVE-2023-22081, CVE-2023-2597, CVE-2023-2727, CVE-2023-2728, CVE-2023-33850
- CVE-2023-35887, CVE-2023-38264, CVE-2023-42503, CVE-2023-43804, CVE-2023-45133
- CVE-2023-45288, CVE-2023-48795, CVE-2023-5676, CVE-2024-10917, CVE-2024-12085
- CVE-2024-12797, CVE-2024-12905, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921
- CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, CVE-2024-21011, CVE-2024-21068

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-2024-21085, CVE-2024-21094, CVE-2024-21131, CVE-2024-21138, CVE-2024-21140
- CVE-2024-21144, CVE-2024-21145, CVE-2024-21147, CVE-2024-21208, CVE-2024-21210
- CVE-2024-21217, CVE-2024-21235, CVE-2024-21626, CVE-2024-21634, CVE-2024-22201
- CVE-2024-23454, CVE-2024-23944, CVE-2024-24790, CVE-2024-24791, CVE-2024-25621
- CVE-2024-25710, CVE-2024-26308, CVE-2024-27267, CVE-2024-28863, CVE-2024-29025
- CVE-2024-29133, CVE-2024-29857, CVE-2024-30171, CVE-2024-30172, CVE-2024-31141
- CVE-2024-3154, CVE-2024-34155, CVE-2024-34447, CVE-2024-35176, CVE-2024-35195
- CVE-2024-3651, CVE-2024-36620, CVE-2024-36621, CVE-2024-36623, CVE-2024-37891
- CVE-2024-38820, CVE-2024-3933, CVE-2024-39908, CVE-2024-40635, CVE-2024-41909
- CVE-2024-43398, CVE-2024-45296, CVE-2024-45336, CVE-2024-45338, CVE-2024-45341
- CVE-2024-47072, CVE-2024-47535, CVE-2024-47875, CVE-2024-48910, CVE-2024-50264
- CVE-2024-50302, CVE-2024-51479, CVE-2024-51744, CVE-2024-52798, CVE-2024-53113
- CVE-2024-55565, CVE-2024-56332, CVE-2024-57980, CVE-2024-6119, CVE-2024-6531
- CVE-2024-7143, CVE-2024-8176, CVE-2024-8184, CVE-2024-9042, CVE-2025-0426
- CVE-2025-13465, CVE-2025-13867, CVE-2025-14689, CVE-2025-15284, CVE-2025-15467
- CVE-2025-1767, CVE-2025-21587, CVE-2025-21613, CVE-2025-21905, CVE-2025-22085
- CVE-2025-22091, CVE-2025-22113, CVE-2025-22121, CVE-2025-22233, CVE-2025-22866
- CVE-2025-22868, CVE-2025-22869, CVE-2025-22870, CVE-2025-22871, CVE-2025-22872
- CVE-2025-24294, CVE-2025-24970, CVE-2025-25193, CVE-2025-2668, CVE-2025-27152
- CVE-2025-27219, CVE-2025-27220, CVE-2025-27221, CVE-2025-27516, CVE-2025-27789
- CVE-2025-27898, CVE-2025-27899, CVE-2025-27900, CVE-2025-27901, CVE-2025-27903
- CVE-2025-27904, CVE-2025-29927, CVE-2025-30691, CVE-2025-30698, CVE-2025-30749
- CVE-2025-30754, CVE-2025-30761, CVE-2025-31133, CVE-2025-32386, CVE-2025-32387
- CVE-2025-32421, CVE-2025-36001, CVE-2025-36009, CVE-2025-36070, CVE-2025-36098
- CVE-2025-36123, CVE-2025-36184, CVE-2025-36247, CVE-2025-36353, CVE-2025-36365
- CVE-2025-36366, CVE-2025-36384, CVE-2025-36387, CVE-2025-36407, CVE-2025-36424
- CVE-2025-36425, CVE-2025-36427, CVE-2025-36428, CVE-2025-36442, CVE-2025-37797
- CVE-2025-37958, CVE-2025-38086, CVE-2025-38089, CVE-2025-38110, CVE-2025-41248
- CVE-2025-41249, CVE-2025-4447, CVE-2025-45582, CVE-2025-4673, CVE-2025-47906
- CVE-2025-47912, CVE-2025-47913, CVE-2025-47935, CVE-2025-47944, CVE-2025-48068
- CVE-2025-48387, CVE-2025-48997, CVE-2025-49128, CVE-2025-50106, CVE-2025-50537
- CVE-2025-5187, CVE-2025-5222, CVE-2025-52565, CVE-2025-52881, CVE-2025-53057
- CVE-2025-53066, CVE-2025-53547, CVE-2025-54410, CVE-2025-55163, CVE-2025-55173
- CVE-2025-55183, CVE-2025-55184, CVE-2025-57752, CVE-2025-57822, CVE-2025-58056
- CVE-2025-58057, CVE-2025-58058, CVE-2025-58183, CVE-2025-58185, CVE-2025-58186
- CVE-2025-58187, CVE-2025-58189, CVE-2025-58190, CVE-2025-58457, CVE-2025-5889
- CVE-2025-59343, CVE-2025-61724, CVE-2025-61727, CVE-2025-61729, CVE-2025-64329
- CVE-2025-64756, CVE-2025-66418, CVE-2025-66471, CVE-2025-66506, CVE-2025-67779
- CVE-2025-6965, CVE-2025-7039, CVE-2025-7338, CVE-2025-7339, CVE-2025-8916
- CVE-2026-1188, CVE-2026-21441, CVE-2026-21925, CVE-2026-21932, CVE-2026-21933
- CVE-2026-21945, CVE-2026-23745, CVE-2026-23950, CVE-2026-24842, CVE-2026-25639
- CVE-2026-25765

Bilan de la vulnérabilité

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

Solution

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

Risque

- Contournement de la politique de sécurité ;
- Déni de service à distance ;
- Exécution de code arbitraire à distance ;
- Injection de code indirecte à distance (XSS) ;
- Élévation de privilèges ;
- Atteinte à l'intégrité des données ;
- Atteinte à la confidentialité des données ;

Annexe

Bulletin de sécurité IBM:

- https://www.ibm.com/support/pages/node/7262324
- https://www.ibm.com/support/pages/node/7262325
- https://www.ibm.com/support/pages/node/7262494
- https://www.ibm.com/support/pages/node/7262548
- https://www.ibm.com/support/pages/node/7262669
- https://www.ibm.com/support/pages/node/7262753
- https://www.ibm.com/support/pages/node/7262754

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