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 IBM
Numéro de Référence	63362004/26
Date de Publication	20 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- API Connect - versions V10.0.8.0 to V10.0.8.7
- Aspera Faspex 5 - versions 5.0.0 to 5.0.15
- DevOps Test Performance - versions 11.0 to 11.0.7
- IBM App Connect Enterprise - multiple versions
- IBM Aspera Console - versions 3.3.0 to 3.4.9
- IBM Aspera Orchestrator - versions 3.0.0 to 4.1.3
- IBM Business Automation Manager Open Editions - versions 8.0.0 to 8.0.8
- IBM Data Product Hub - versions 5.0.0 to 5.3.1
- IBM Event Processing - versions 1.0.0 to 1.4.7
- IBM Guardium Data Protection - versions 12.0, 12.1 et 12.2
- IBM Maximo Application Suite - Monitor Component - multiple versions
- IBM Netezza Appliance - versions 1.0.0.0 et 1.0.0.1
- IBM SPSS Modeler - multiple versions
- IBM Tivoli Network Configuration Manager (ITNCM) - versions 6.4.2 to 6.4.2 Fix Pack 23
- IBM Watson Speech Services Cartridge - versions 4.0.0 to 5.3.1
- IBM watsonx Orchestrate Cartridge pour IBM Cloud Pak pour Data - multiple versions
- Performance Tester (RPT) - versions 11.0 to 11.0.7
- Rational Performance Tester - multiple versions
- SPSS Collaboration et Deployment Services - version 9.0.0.0

Identificateurs externes

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-2025-12635 CVE-2025-14923 CVE-2025-69873 CVE-2026-1615 CVE-2026-2359
- CVE-2026-24001 CVE-2026-29063 CVE-2026-31808 CVE-2026-3304 CVE-2026-3520
- CVE-2025-61729 CVE-2024-29371 CVE-2025-68973 CVE-2025-61727 CVE-2025-6176
- CVE-2025-14914 CVE-2025-66506 CVE-2025-58188 CVE-2025-58187 CVE-2026-33186
- CVE-2025-22874 CVE-2025-9784 CVE-2025-47911 CVE-2025-47907 CVE-2025-48924
- CVE-2025-15366 CVE-2026-22772 CVE-2019-1010266

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits IBM susmentionnées. L'exploitation de ces failles pourrait permettre à un attaquant d'élever ses privilèges, d'exécuter du code arbitraire à distance, de contourner des mécanismes de sécurité, de provoquer un déni de service, de divulguer des informations sensibles ou encore de réussir une usurpation d'identité.

Solution :

Veuillez se référer au bulletin de sécurité IBM du 20 Avril 2026 pour plus d'infirmation.

Risque :

- Élévation des privilèges ;
- Déni de service ;
- Divulgation d'informations confidentielles ;
- Exécution de code arbitraire à distance ;
- Contournement de la politique de sécurité ;
- Usurpation d'identité ;

Annexe

Bulletin de sécurité IBM du 20 Avril 2026**:**

- https://www.ibm.com/support/pages/bulletin/