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 Atlassian
Numéro de Référence	62211903/26
Date de Publication	19 Mars 2026
Risque	Important
Impact	Important

Systèmes affectés

- BamboData Center et Server versions antérieures à :
  - 12.1.3 (LTS) recommandée Data Center uniquement
  - 10.2.16 (LTS) Data Center uniquement
  - 9.6.24 (LTS) Data Center uniquement
- Bitbucket Data Center et Server versions antérieures à :
  - 10.2.1 (LTS) recommandée Data Center uniquement
  - 10.1.5 Data Center uniquement
  - 9.4.18 (LTS) Data Center uniquement
- Confluence Server et Confluence Data Center versions antérieures à :
  - 10.2.7 (LTS) recommandée Data Center uniquement
  - 9.2.17 (LTS) Data Center uniquement
  - 9.0.3 Data Center uniquement
- Crowd Server et Crowd Data Center versions antérieures à :
  - 7.1.5 recommandée Data Center uniquement
  - 6.3.5 Data Center uniquement
- Fisheye/Crucible versions antérieures à :
  - 4.9.8 recommandée
- Jira Data Center et Server versions antérieures à :
  - 11.3.3 (LTS) recommandée Data Center uniquement
  - 10.3.18 (LTS) Data Center uniquement

- Jira Service Management Data Center et Server versions antérieures à :
    - 11.3.3 (LTS) recommandée Data Center uniquement
    - 10.3.18 (LTS) Data Center uniquement

Identificateurs externes

- CVE-2026-21570 CVE-2025-68493 CVE-2025-64775 CVE-2022-25883 CVE-2025-64756
- CVE-2026-21884 CVE-2026-22029 CVE-2026-25639 CVE-2023-52428 CVE-2026-23950
- CVE-2026-23745 CVE-2026-24842 CVE-2022-25927 CVE-2022-25883 CVE-2020-28469
- CVE-2026-23950 CVE-2026-23745 CVE-2026-24842 CVE-2024-57699 CVE-2022-25927
- CVE-2020-28469

Bilan de la vulnérabilité

Atlassian a publié des mises à jour de sécurité corrigeant plusieurs vulnérabilités affectant les produits susmentionnés. L'exploitation de ces failles pourrait permettre à des attaquants de provoquer des attaques par déni de service (DoS), d'exécuter du code arbitraire à distance, d'injecter des commandes système, d'exploiter des traversées de répertoires, ou encore de compromettre la confidentialité et l'intégrité des données, ainsi de contourner les mécanismes de sécurité.

Solution :

Veuillez se référer au bulletin de sécurité Atlassian du 17 Mars 2026 pour plus d'infirmation.

Risque :

- Déni de service
- Exécution du code arbitraire à distance
- Injection des commandes système
- Traversée de répertoire
- Contournement de la politique de sécurité
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité Atlassian du 17 Mars 2026**:**

- https://confluence.atlassian.com/security/security-bulletin-march-17-2026-1721271371.html