

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
.....
مركز اليقظة والرصد والتصدي
للتهجمات المعلوماتية

.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits Atlassian
Numéro de Référence	60252201/26
Date de Publication	22 janvier 2026
Risque	Important
Impact	Critique

Systèmes affectés

- Bamboo Data Center and Server 12.0.0 à 12.0.1
- Bamboo Data Center and Server 11.0.0 à 11.0.8
- Bamboo Data Center and Server 10.2.0 à 10.2.12 (LTS)
- Bamboo Data Center and Server 10.1.0 à 10.1.1
- Bamboo Data Center and Server 10.0.0 à 10.0.3
- Bamboo Data Center and Server 9.6.0 à 9.6.20 (LTS)
- Bitbucket Data Center and Server 10.0.0 à 10.0.2
- Bitbucket Data Center and Server 9.6.0 à 9.6.5
- Bitbucket Data Center and Server 9.5.0 à 9.5.2
- Bitbucket Data Center and Server 9.4.0 à 9.4.14 (LTS)
- Bitbucket Data Center and Server 9.3.0 à 9.3.2
- Bitbucket Data Center and Server 9.2.0 à 9.2.1
- Bitbucket Data Center and Server 9.1.0 à 9.1.1
- Bitbucket Data Center and Server 9.0.1
- Bitbucket Data Center and Server 8.19.0 à 8.19.25 (LTS)
- Bitbucket Data Center and Server 8.18.0 à 8.18.1
- Confluence Data Center and Server 10.2.0 à 10.2.1 (LTS)
- Confluence Data Center and Server 10.1.0 à 10.1.2
- Confluence Data Center and Server 10.0.2 à 10.0.3
- Confluence Data Center and Server 9.5.1 à 9.5.4
- Confluence Data Center and Server 9.4.0 à 9.4.1

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques
Informatiques
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 للتهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني: contact@macert.gov.ma

- Confluence Data Center and Server 9.3.1 à 9.3.2
- Confluence Data Center and Server 9.2.0 à 9.2.12 (LTS)
- Confluence Data Center and Server 9.1.0 à 9.1.1
- Confluence Data Center and Server 9.0.1 à 9.0.3
- Confluence Data Center and Server 8.9.0 à 8.9.8
- Confluence Data Center and Server 8.8.0 à 8.8.1
- Confluence Data Center and Server 8.5.6 à 8.5.31 (LTS)
- Confluence Data Center and Server 7.19.19 à 7.19.30 (LTS)
- Crowd Data Center and Server 7.1.0 à 7.1.2
- Crowd Data Center and Server 6.3.0 à 6.3.3
- Jira Data Center and Server 11.2.0
- Jira Data Center and Server 11.1.0 à 11.1.1
- Jira Data Center and Server 11.0.0 à 11.0.1
- Jira Data Center and Server 10.7.1 à 10.7.4
- Jira Data Center and Server 10.6.0 à 10.6.1
- Jira Data Center and Server 10.5.0 à 10.5.1
- Jira Data Center and Server 10.4.0 à 10.4.1
- Jira Data Center and Server 10.3.0 à 10.3.15 (LTS)
- Jira Data Center and Server 10.2.0 à 10.2.1
- Jira Data Center and Server 10.1.1 à 10.1.2
- Jira Data Center and Server 10.0.0 à 10.0.1
- Jira Data Center and Server 9.17.0 à 9.17.5
- Jira Data Center and Server 9.16.0 à 9.16.1
- Jira Data Center and Server 9.15.2
- Jira Data Center and Server 9.14.0 à 9.14.1
- Jira Data Center and Server 9.13.0 à 9.13.1
- Jira Data Center and Server 9.12.3 à 9.12.25 (LTS)
- Jira Service Management Data Center and Server 11.3.0 (LTS)
- Jira Service Management Data Center and Server 11.2.0
- Jira Service Management Data Center and Server 11.1.0 to 11.1.1
- Jira Service Management Data Center and Server 11.0.0 to 11.0.1
- Jira Service Management Data Center and Server 10.7.1 to 10.7.4
- Jira Service Management Data Center and Server 10.6.0 to 10.6.1
- Jira Service Management Data Center and Server 10.5.0 to 10.5.1
- Jira Service Management Data Center and Server 10.4.0 to 10.4.1
- Jira Service Management Data Center and Server 10.3.0 to 10.3.15 (LTS)
- Jira Service Management Data Center and Server 10.2.0 to 10.2.1
- Jira Service Management Data Center and Server 10.1.1 to 10.1.2
- Jira Service Management Data Center and Server 10.0.0 to 10.0.1
- Jira Service Management Data Center and Server 5.17.0 to 5.17.5
- Jira Service Management Data Center and Server 5.16.0 to 5.16.1
- Jira Service Management Data Center and Server 5.15.2
- Jira Service Management Data Center and Server 5.14.0 to 5.14.1
- Jira Service Management Data Center and Server 5.13.0 to 5.13.1

- Jira Service Management Data Center and Server 5.12.3 to 5.12.28 (LTS)

Identificateurs externes

CVE-2021-3807 CVE-2022-25883 CVE-2024-45296 CVE-2024-45801 CVE-2025-12383
CVE-2025-15284 CVE-2025-41249 CVE-2025-49146 CVE-2025-52434 CVE-2025-53689
CVE-2025-55752 CVE-2025-64775 CVE-2025-9287 CVE-2025-9288 CVE-2026-21569

Bilan de la vulnérabilité

Atlassian annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire d'accéder à des données confidentielles ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité d'Atlassian pour installer les mises à jour.

Risques

- Exécution de code arbitraire
- Accès à des données confidentielles
- Déni de service

Références

Bulletin de sécurité d'Atlassian:

- <https://confluence.atlassian.com/security/security-bulletin-january-20-2026-1712324819.html>