# ROYAUME DU MAROC ADMINISTRATION DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

mtro do Voillo do Dóto

Centre de Veille de Détection et de Réaction aux Attaques Informatiques



المملكة المغربية إدارة الدفاع الوطني المديرية العامة الأمن نظم المعلومات مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

#### **BULLETIN DE SECURITE**

Titre	Vulnérabilités affectant des produits Atlassian
Numéro de Référence	57702210/25
Date de Publication	22 octobre 2025
Risque	Important
Impact	Important

## Systèmes affectés

- Jira Data Center versions antérieures à la version 11.1.0
- Jira Data Center versions antérieures à la version 10.3.12 (LTS)
- Jira Data Center and Server versions antérieures à la version 9.12.28 (LTS)
- Bamboo Data Center versions antérieures à la version 11.0.5
- Bamboo Data Center versions antérieures à la version 10.2.8 (LTS)
- Bamboo Data Center versions antérieures à la version 9.6.17 (LTS)
- Fisheye/Crucible versions antérieures à 4.9.3
- Jira Service Management Data Center versions antérieures à la version 11.1.0
- Jira Service Management Data Center versions antérieures à la version 10.3.12 (LTS)
- Jira Service Management Data Center and Server versions antérieures à la version 5.12.28 (LTS)

#### **Identificateurs externes**

CVE-2025-7962 CVE-2025-58057 CVE-2025-58056 CVE-2025-48989 CVE-2025-48976 CVE-2025-22167 CVE-2023-46604 CVE-2023-22527 CVE-2023-22524 CVE-2023-22523 CVE-2023-22518 CVE-2022-41903 CVE-2022-31692 CVE-2022-23521 CVE-2022-22978 CVE-2022-22965 CVE-2022-1471 CVE-2019-13990

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 للهجمات المعلوماتية هاتف: 47 37 37 37 05 05 ماكس: 53 27 37 75 05 05 البريد الإلكتروني contact@macert.gov.ma

#### 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'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

- Accès à des données confidentielles
- Déni de service

## Références

Bulletin de sécurité d'Atlassian:

• <a href="https://confluence.atlassian.com/security/security-bulletin-october-21-2025-1652920034.html">https://confluence.atlassian.com/security/security-bulletin-october-21-2025-1652920034.html</a>

Tél: 05 37 57 21 47 - Fax: 05 37 57 20 53

Email: contact@macert.gov.ma