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	58631911/25
Date de Publication	19 Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Jira Software Server versions antérieures à 9.12.26
- Jira Software Server versions antérieures à 11.2.0
- Jira Software Server versions antérieures à 10.7.3
- Jira Software Server versions antérieures à 10.3.10
- Jira Software Data Center versions antérieures à 9.12.26
- Jira Software Data Center versions antérieures à 11.2.0
- Jira Software Data Center versions antérieures à 10.7.3
- Jira Software Data Center versions antérieures à 10.3.10
- Jira Service Management Server versions antérieures à 5.12.26
- Jira Service Management Server versions antérieures à 11.2.0
- Jira Service Management Server versions antérieures à 10.7.3
- Jira Service Management Server versions antérieures à 10.3.10
- Jira Service Management Data Center versions antérieures à 5.12.26
- Jira Service Management Data Center versions antérieures à 11.2.0
- Jira Service Management Data Center versions antérieures à 10.7.3
- Jira Service Management Data Center versions antérieures à 10.3.10
- Confluence Server versions antérieures à 9.5.4
- Confluence Server versions antérieures à 9.4.0
- Confluence Server versions antérieures à 9.3.1

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

- Confluence Server versions antérieures à 9.2.6
- Confluence Server versions antérieures à 8.5.20
- Confluence Server versions antérieures à 10.1.1
- Confluence Server versions antérieures à 10.0.2
- Confluence Data Center versions antérieures à 9.5.4
- Confluence Data Center versions antérieures à 9.4.0
- Confluence Data Center versions antérieures à 9.3.1
- Confluence Data Center versions antérieures à 9.2.6
- Confluence Data Center versions antérieures à 8.5.20
- Confluence Data Center versions antérieures à 10.1.1
- Confluence Data Center versions antérieures à 10.0.2

Identificateurs externes

- CVE-2022-38900 CVE-2022-46175 CVE-2023-42282 CVE-2024-37890
- CVE-2024-45296 CVE-2025-41248 CVE-2025-48387 CVE-2025-48976

Bilan de la vulnérabilité

Atlassian a publié des mises à jour de sécurité corrigeant plusieurs vulnérabilités affectant les produits susmentionnés. L'exploitation réussie de ces failles peut entraîner des attaques par déni de service (DoS), une exécution du code arbitraire à distance, une atteinte à la confidentialité et l'intégrité des données ou un contournement de la politique de sécurité.

Solution :

Veuillez se référer au bulletin de sécurité Atlassian du 18 Novembre 2025 pour plus d'infirmation.

Risque :

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

Annexe

Bulletin de sécurité Atlassian du 18 Novembre 2025**:**

- https://jira.atlassian.com/browse/JSWSERVER-26537

- https://jira.atlassian.com/browse/JSDSERVER-16435
- https://jira.atlassian.com/browse/CONFSERVER-101488
- https://jira.atlassian.com/browse/CONFSERVER-101487
- https://jira.atlassian.com/browse/CONFSERVER-101486
- https://jira.atlassian.com/browse/CONFSERVER-101485
- https://jira.atlassian.com/browse/CONFSERVER-101480
- https://jira.atlassian.com/browse/CONFSERVER-101479
- https://jira.atlassian.com/browse/CONFSERVER-101477