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	55871707/25
Date de Publication	17 Juillet 2025
Risque	Important
Impact	Important

Systèmes affectés

- Bamboo 11.0.3 (édition Data Center uniquement)
- Bamboo 10.2.6 (LTS – édition Data Center uniquement)
- Bamboo 9.6.15 (LTS – édition Data Center uniquement)
- Bitbucket 9.6.4 (édition Data Center uniquement)
- Bitbucket 9.4.8 (LTS – édition Data Center uniquement)
- Bitbucket 8.19.20 (LTS – édition Data Center uniquement)
- Jira Service Management Data Center versions 10.x antérieures à 10.7.2
- Jira Service Management Data Center versions 5.x antérieures à 5.12.25 LTS
- Jira Service Management Data Center versions antérieures à 10.3.8 LTS
- Jira Service Management Server versions 10.x antérieures à 10.3.8 LTS
- Jira Service Management Server versions 10.x antérieures à 10.7.2
- Jira Service Management Server versions 5.x antérieures à 5.12.25 LTS
- Jira Software Data Center versions 10.x antérieures à 10.3.8 LTS
- Jira Software Data Center versions 10.x antérieures à 10.7.2
- Jira Software Data Center versions 9.x antérieures à 9.12.25 LTS
- Jira Software Server versions 10.x antérieures à 10.3.8 LTS
- Jira Software Server versions 10.x antérieures à 10.7.2
- Jira Software Server versions 9.x antérieures à 9.12.25 LTS
- Confluence Data Center versions 9.x antérieures à 9.5.2

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 Data Center versions 9.x antérieures à 9.2.6 LTS
- Confluence Server versions 9.x antérieures à 9.2.6 LTS
- Confluence Server versions 9.x antérieures à 9.5.2
- Crowd Data Center et Server versions antérieures à 5.2.11

Identificateurs externes

- CVE-2017-1000034 CVE-2024-13009 CVE-2024-45801 CVE-2024-45801
- CVE-2025-22228 CVE-2025-22228 CVE-2025-27820 CVE-2025-27820
- CVE-2025-27820 CVE-2025-27820 CVE-2025-46701 CVE-2025-46701
- CVE-2025-46701 CVE-2025-48734 CVE-2025-48976 CVE-2025-48988
- CVE-2025-48988 CVE-2025-49125 CVE-2025-49125 CVE-2025-49146

Bilan de la vulnérabilité

Atlassian a publié des mises à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation réussie de ces failles peut entraîner des attaques par déni de service (DoS), 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 16 Juillet 2025 pour plus d'infirmation.

Risque :

- Déni de service
- Contournement de la politique de sécurité
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité Atlassian du 16 Juillet 2025**:**

- https://confluence.atlassian.com/security/security-bulletin-july-15-2025-1590658642.html