ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

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

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant des produits Atlassian
Numéro de Référence	59261212/25
Date de Publication	12 décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Bamboo Data Center 12.0.1
- Bamboo Data Center 10.2.0 à 10.2.11 (LTS)
- Bamboo Data Center 9.6.1 à 9.6.19 (LTS)
- Bitbucket Datacenter 9.1.0 à 9.1.1
- Bitbucket Datacenter 9.0.1
- Bitbucket Datacenter 8.19.0 à 8.19.24(LTS)
- Bitbucket Datacenter 8.18.0 à 8.18.1
- Confluence Data Center 10.2.0 (LTS)
- Confluence Data Center 10.1.0 à 10.1.2
- Confluence Data Center 10.0.2 à 10.0.3
- Confluence Data Center 9.5.1 à 9.5.4
- Confluence Data Center 9.4.0 à 9.4.1
- Confluence Data Center 9.3.1 à 9.3.2
- Confluence Data Center 9.2.0 à 9.2.11 (LTS)
- Confluence Data Center 9.1.0 à 9.1.1
- Confluence Data Center 9.0.1 à 9.0.3
- Confluence Data Center 8.9.0 à 8.9.8
- Confluence Data Center 8.8.0 à 8.8.1
- Confluence Data Center and Server 8.5.5 à 8.5.29 (LTS)
- Confluence Data Center and Server 7.19.18 à 7.19.30 (LTS)
- Crowd Data Center 7.1.0 à 7.1.1

- Crowd Data Center 7.0.0 à 7.0.2
- Crowd Data Center 6.3.0 à 6.3.3
- Crowd Data Center 6.2.0 à 6.2.6
- Crowd Data Center 6.1.0 à 6.1.7
- Crowd Data Center 6.0.0 à 6.0.10
- Crowd Data Center 5.3.0 à 5.3.8
- Crowd Data Center 5.2.2 à 5.2.11
- Crowd Data Center 5.1.7 à 5.1.13
- Fisheye/Crucible 4.9.0 à 4.9.5
- Fisheye/Crucible 4.8.14 à 4.8.16
- Jira Data Center 11.2.0 à 11.2.1
- Jira Data Center 11.1.0 à 11.1.1
- Jira Data Center 11.0.0 à 11.0.1
- Jira Data Center 10.3.0 à 10.3.14 (LTS)
- Jira Data Center 9.12.1 à 9.12.30 (LTS)
- Jira Service Management Data Center 11.2.0 à 11.2.1
- Jira Service Management Data Center 11.1.0 à 11.1.1
- Jira Service Management Data Center 11.0.0 à 11.0.1
- Jira Service Management Data Center 10.3.0 à 10.3.14 (LTS)

Identificateurs externes

CVE-2016-1181 CVE-2016-1182 CVE-2019-13990 CVE-2020-36518 CVE-2020-8203 CVE-2021-39227 CVE-2021-46877 CVE-2022-1471 CVE-2022-22965 CVE-2022-22978 CVE-2022-23521 CVE-2022-31692 CVE-2022-3517 CVE-2022-37599 CVE-2022-37601 CVE-2022-37603 CVE-2022-41903 CVE-2022-42004 CVE-2022-45693 CVE-2023-22518 CVE-2023-22522 CVE-2023-22523 CVE-2023-22524 CVE-2023-22527 CVE-2023-46604 CVE-2023-49735 CVE-2024-12905 CVE-2024-13009 CVE-2024-21634 CVE-2024-29415 CVE-2024-7254 CVE-2025-27152 CVE-2025-41248 CVE-2025-48976 CVE-2025-48989 CVE-2025-52434 CVE-2025-52999 CVE-2025-54988 CVE-2025-55163 CVE-2025-58754 CVE-2025-59250 CVE-2025-66516

Bilan de la vulnérabilité

Atlassian annonce la correction de plusieurs vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance, d'injecter des entités XML Externe (XXE) ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité d'Atlassian pour installer les mises à jour.

Risques

- Exécution de code arbitraire à distance
- injection d'entités XML Externe (XXE)
- Déni de service

Références

Bulletin de sécurité d'Atlassian:

- https://confluence.atlassian.com/security/security-bulletin-december-11-2025-1689616574.html