مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Atlassian

Tracking #:432318288

Date:21-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that has Atlassian has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Atlassian has released its January 2026 security updates addressing multiple critical and high-severity vulnerabilities affecting Bamboo, Bitbucket, Confluence, Crowd, Jira Software, and Jira Service Management for Data Center and Server deployments.

The vulnerabilities originate mainly from third-party dependencies and may lead to denial of service, XML external entity (XXE) injection, server-side request forgery (SSRF), man-in-the-middle (MITM) attacks, cross-site scripting (XSS), improper authorization, and remote code execution (RCE).

Vulnerability Details
Critical Severity

- **CVE-2025-12383** – Race condition in jersey-client (Bamboo) – CVSS 9.4
- **CVE-2025-66516** – XXE vulnerability in Confluence dependency – CVSS 10.0

High Severity

- **CVE-2025-54988** – XXE in org.apache.tika:tika-core (Bamboo, Confluence, Crowd)
- **CVE-2025-55163** – DoS in io.netty:netty-codec-http2 (Bamboo)
- **CVE-2025-27152** – SSRF in axios (Bamboo)
- **CVE-2025-52999** – DoS in jackson-core (Bitbucket)
- **CVE-2024-38286** – DoS in Apache Tomcat (Bitbucket)
- **CVE-2025-48989** – DoS in Apache Tomcat (Bitbucket)
- **CVE-2025-55752** – Remote code execution in Apache Tomcat (Bitbucket)
- **CVE-2025-41249** – Improper authorization in Spring Core (Bitbucket)
- **CVE-2025-53689** – XXE in Apache Jackrabbit (Confluence)
- **CVE-2025-49146** – MITM in PostgreSQL JDBC driver (Confluence)
- **CVE-2026-21569** – XXE vulnerability (Crowd)
- **CVE-2025-48976** – DoS in Commons FileUpload (Crowd)
- **CVE-2025-64775** – DoS in Apache Struts (Crowd)
- **CVE-2025-15284** – DoS in qs dependency (Jira, JSM)
- **CVE-2025-52434** – DoS in tomcat-coyote (Jira, JSM)
- **CVE-2024-21538** – DoS in cross-spawn (Jira, JSM)
- **CVE-2021-3807** – DoS in ansi-regex (Jira, JSM)
- **CVE-2025-9288** – Injection in sha.js (Jira, JSM)
- **CVE-2025-9287** – Injection in cipher-base (Jira, JSM)
- **CVE-2024-45801** – Cross-site scripting in dompurify (Jira, JSM)
- **CVE-2022-25883** – DoS in semver (JSM)
- **CVE-2024-45296** – DoS in path-to-regexp (JSM)
- **CVE-2022-45693** – DoS in org.codehaus.jettison:jettison (JSM)

Fixed Versions:
Bamboo Data Center and Server

- 12.0.2
- 10.2.13 to 10.2.14 (LTS)
- 9.6.21 to 9.6.22 (LTS)

Bitbucket Data Center and Server

- 10.1.1 to 10.1.4
- 9.4.15 to 9.4.16 (LTS)
- 8.19.26 to 8.19.27 (LTS)

Confluence Data Center and Server

- 10.2.2 (LTS)
- 9.2.13 (LTS)

Crowd Data Center and Server

- 7.1.3
- 6.3.4

Jira Data Center and Server

- 11.3.0 to 11.3.1 (LTS)
- 11.2.1
- 10.3.16 (LTS)
- 9.12.26 to 9.12.31 (LTS)

Jira Service Management Data Center and Server

- 11.3.0 to 11.3.1 (LTS)
- 11.2.1
- 10.3.16 (LTS)
- 5.12.29 to 5.12.31 (LTS)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Atlassian.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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