مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Atlassian November 2025 Security Updates

Tracking #:432318032

Date:19-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Atlassian released its monthly Security Bulletin detailing 39 newly disclosed vulnerabilities, consisting of 5 Critical and 34 High-severity issues.

TECHNICAL DETAILS:

Atlassian released its monthly Security Bulletin detailing 39 newly disclosed vulnerabilities, consisting of 5 Critical and 34 High-severity issues. These vulnerabilities affect multiple Atlassian Data Center and Server products including Bitbucket, Confluence, Jira Software, and Jira Service Management.

Most vulnerabilities stem from third-party dependencies, but still pose elevated security risks including Remote Code Execution (RCE), Server-Side Request Forgery (SSRF), Denial of Service (DoS), Improper Authorization, Path Traversal, Prototype Pollution, Cryptographic Failures, and Broken Authentication.

Atlassian strongly recommends immediate patching to the latest fixed versions to mitigate these risks. While many issues are assessed as lower-risk due to Atlassian's integration context, several CVEs possess high CVSS scores, indicating potential severe impact in unpatched environments.

Details of Vulnerabilities

1. Affected Products

The following Atlassian products are impacted:

- Bitbucket Data Center & Server
- Confluence Data Center & Server
- Jira Software Data Center & Server
- Jira Service Management Data Center & Server

Each product has specific affected and fixed versions as outlined by Atlassian.

2. Critical Vulnerabilities (CVSS 9.3 – 10)

RCE – Bitbucket (Third-Party Dependency)

- CVE-2024-38999 – CVSS 10.0 Critical
- CVE-2016-1000027 – CVSS 9.8 Critical
- CVE-2023-42282 – CVSS 9.8 Critical (SSRF)
- CVE-2023-45133 – CVSS 9.3 Critical

3. High-Severity Vulnerabilities (CVSS 7.1 – 8.8)

In Bitbucket Data Center & Server

High-severity issues include:

- Improper Authorization (e.g., CVE-2025-48734, CVE-2025-41248)
- Denial of Service across many dependencies (CVE-2025-55163, CVE-2024-25710, CVE-2023-52428, etc.)
- Path Traversal (CVE-2022-24785, CVE-2024-38819)
- Cryptographic Failures (CVE-2022-24771, CVE-2022-24772)
- Prototype Pollution (CVE-2020-8203, CVE-2020-28471)
- Command Injection (CVE-2021-23337)
- Broken Authentication (CVE-2025-22228)

In Confluence Data Center & Server
Key vulnerabilities include:

- SSRF (CVE-2023-42282 – 9.8 Critical)
- Path Traversal (CVE-2025-48387)
- DoS (CVE-2025-22166, CVE-2024-37890, others)
- Improper Authorization (CVE-2025-41248)
- Prototype Pollution (CVE-2022-46175)

In Jira Software & Jira Service Management
Both products are affected by:

- CVE-2025-48976 – DoS – CVSS 7.5 High

Fixed Versions:
Bitbucket

- 10.0.2 (DC only)
- 8.19.25 (LTS, DC only)
- 9.4.13 (LTS recommended)

Confluence

- 10.1.1 (DC only)
- 10.0.2–10.0.3 (DC only)
- 9.2.7 to 9.2.10 (LTS) recommended Data Center Only
- 8.5.25 to 8.5.28 (LTS)

Jira Software

- 11.2.0 (DC only)
- 10.7.3–10.7.4
- 10.3.10–10.3.13 (LTS)
- 9.12.26 to 9.12.29 (LTS)

Jira Service Management

- 11.2.0 (DC only)
- 10.7.3–10.7.4
- 10.3.10–10.3.13 (LTS)
- 5.12.26–5.12.29 (LTS)

RECOMMENDATIONS:

- Apply Atlassian Patch Versions Immediately: Upgrade all products to the latest fixed versions, as listed in the bulletin.

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-november-18-2025-1671463469.html