

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Bulletin- Atlassian Products

Tracking #:432317495

Date:17-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Atlassian has released its July 2025 Security Bulletin, detailing 20 high-severity vulnerabilities across major products, including Jira, Confluence, Bitbucket, Bamboo, Crowd, and Jira Service Management.

TECHNICAL DETAILS:

Atlassian has released its July 2025 Security Bulletin, detailing 20 high-severity vulnerabilities across major products, including Jira, Confluence, Bitbucket, Bamboo, Crowd, and Jira Service Management. These vulnerabilities affect multiple third-party dependencies and core components, exposing systems to Remote Code Execution (RCE), Denial of Service (DoS), Man-in-the-Middle (MITM) attacks, Cross-Site Scripting (XSS), and Broken Authentication and Session Management (BASM).

All users of Atlassian **Data Center and Server** deployments are strongly advised to update to the **fixed versions** immediately to reduce risk exposure. While these issues are not part of Atlassian's Critical Security Advisories, their high CVSS scores (up to 8.8) warrant immediate remediation.

Vulnerability Details and Affected Products:

1. Bamboo Data Center and Server

- **Vulnerabilities:** RCE, DoS, Third-Party Issues
- **CVEs:** CVE-2025-48734 (RCE, CVSS 8.8), CVE-2025-49146, CVE-2025-48976, CVE-2025-27820, CVE-2024-13009
- **Fixed Versions:** 11.0.3, 10.2.6 (LTS), 9.6.15 (LTS)

2. Bitbucket Data Center and Server

- **Vulnerability:** Improper Authorization in tomcat-embed-core
- **CVE:** CVE-2025-46701 (CVSS 7.3)
- **Fixed Versions:** 9.6.4, 9.4.8 (LTS), 8.19.20 (LTS)

3. Confluence Data Center and Server

- **Vulnerability:** MITM in httpclient5
- **CVE:** CVE-2025-27820 (CVSS 7.5)
- **Fixed Versions:** 9.5.2, 9.2.6 (LTS)

4. Crowd Data Center and Server

- **Vulnerability:** RCE in akka-actor
- **CVE:** CVE-2017-1000034 (CVSS 8.1)
- **Fixed Version:** 5.2.11

5. Jira Data Center and Server

- **Vulnerabilities:**
 - XSS in DOMPurify (CVE-2024-45801, CVSS 7.3)
 - MITM in httpclient5 (CVE-2025-27820, CVSS 7.5)
 - DoS, BASM, Improper Authorization in tomcat-catalina, spring-security-crypto
- **CVEs:** CVE-2025-48988, CVE-2025-49125, CVE-2025-22228, CVE-2025-46701
- **Fixed Versions:** 10.7.2, 10.3.8 (LTS), 9.12.25 (LTS)

6. Jira Service Management Data Center and Server

- **CVEs:** CVE-2025-48988, CVE-2025-49125, CVE-2025-22228, CVE-2025-46701
- **Fixed Versions:** 10.7.2, 10.3.8 (LTS), 5.12.25 (LTS)

RECOMMENDATIONS:

- Patch Immediately: Upgrade to the recommended Fixed Versions listed above for each product.

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-july-15-2025-1590658642.html>