مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates - Atlassian

Tracking #:432319147

Date:17-06-2026

## EXECUTIVE SUMMARY:

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

## TECHNICAL DETAILS:

Atlassian has released its June 2026 security updates to address multiple vulnerabilities affecting Bamboo, Bitbucket, Confluence, Crowd, Fisheye/Crucible, Jira Software, and Jira Service Management. The vulnerabilities primarily originate from third-party dependencies used within Atlassian products. Successful exploitation could result in remote code execution (RCE), authentication bypass, server-side request forgery (SSRF), injection attacks, HTTP request smuggling, information disclosure, and denial-of-service (DoS) conditions.

**Vulnerability Details**

**Critical-Severity:**

- CVE-2026-42043 SSRF (Server-Side Request Forgery) axios Dependency in Jira Software / Jira Service Management Data Center (CVSS: 10.0)
- CVE-2026-40175 Prototype Pollution axios Dependency in Jira Software / Jira Service Management Data Center and Server (CVSS: 10.0)
- CVE-2026-41293 Injection org.apache.tomcat:tomcat-coyote Dependency in Confluence / Jira Software Data Center (CVSS: 9.8)
- CVE-2026-43512 BASM (Broken Authentication & Session Management) / Authentication Bypass org.apache.tomcat:tomcat-catalina Dependency in Confluence / Jira Software / Jira Service Management Data Center (CVSS: 9.8)
- CVE-2026-42581 HTTP Request Smuggling io.netty:netty-codec-http Dependency in Crowd Data Center (CVSS: 9.8)
- CVE-2026-22732 Business Logic Vulnerability org.springframework.security:spring-security-web Dependency in Crowd Data Center (CVSS: 9.1)
- CVE-2026-42584 HTTP Request Smuggling io.netty:netty-codec-http Dependency in Crowd / Confluence Data Center (CVSS: 9.1)
- CVE-2026-42579 Injection io.netty:netty-codec-dns Dependency in Confluence Data Center (CVSS: 9.1)
- CVE-2026-43515 Improper Authorization org.apache.tomcat:tomcat-catalina / tomcat-coyote Dependency in Confluence / Jira Software / Jira Service Management Data Center (CVSS: 9.1)
- CVE-2026-42264 Injection axios Dependency in Jira Software / Jira Service Management Data Center (CVSS: 9.1)
- CVE-2026-41293 Injection org.apache.tomcat:tomcat-catalina Dependency in Jira Software Data Center (CVSS: 9.8)

**High-Severity:**

- CVE-2026-41044 RCE (Remote Code Execution) org.apache.activemq:activemq-broker Dependency in Bamboo Data Center (CVSS: 8.8)
- CVE-2026-26996 DoS (Denial of Service) minimatch Dependency in Confluence Data Center (CVSS: 8.7)
- CVE-2026-33871 DoS (Denial of Service) io.netty:netty-codec-http2 Dependency in Jira Service Management Data Center (CVSS: 8.7)
- CVE-2026-44492 SSRF (Server-Side Request Forgery) axios Dependency in Bamboo Data Center (CVSS: 8.6)

- CVE-2026-44487 Information Disclosure axios Dependency in Bamboo Data Center (CVSS: 8.2)
- CVE-2026-42211 RCE (Remote Code Execution) react-router Dependency in Jira Software / Jira Service Management Data Center (CVSS: 8.1)
- CVE-2026-45149 DoS (Denial of Service) @isaacs/brace-expansion Dependency in Bitbucket / Confluence Data Center (CVSS: 7.5)
- CVE-2026-41284 DoS (Denial of Service) org.apache.tomcat:tomcat-catalina Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-42038 SSRF (Server-Side Request Forgery) axios Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-42033 Injection axios Dependency in multiple Atlassian products (CVSS: 7.4)
- CVE-2026-42035 Injection axios Dependency in multiple Atlassian products (CVSS: 7.4)
- CVE-2026-44495 RCE (Remote Code Execution) axios Dependency in Jira Software / Jira Service Management Data Center (CVSS: 7.0)
- CVE-2026-42585 HTTP Request Smuggling io.netty:netty-codec-http Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-42583 DoS (Denial of Service) io.netty:netty-codec Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-44486 Information Disclosure axios Dependency in Bamboo Data Center (CVSS: 7.5)
- CVE-2026-44488 DoS (Denial of Service) axios Dependency in Bamboo Data Center (CVSS: 7.5)
- CVE-2026-44496 DoS (Denial of Service) axios Dependency in Bamboo Data Center (CVSS: 7.5)
- CVE-2026-43513 Business Logic Vulnerability Apache Tomcat Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-27903 DoS (Denial of Service) minimatch Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-27904 DoS (Denial of Service) minimatch Dependency in multiple Atlassian products (CVSS: 7.5)
- CVE-2026-42498 Information Disclosure tomcat-websocket Dependency in Confluence / Jira Software Data Center (CVSS: 7.3)
- CVE-2026-33870 HTTP Request Smuggling io.netty:netty-codec-http Dependency in Jira / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-34487 Information Disclosure tomcat-catalina Dependency in Jira / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-34486 Cryptographic Failure tomcat-catalina Dependency in Jira / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-29129 Cryptographic Failure tomcat-catalina Dependency in Jira Service Management Data Center (CVSS: 7.5)
- CVE-2021-3803 DoS (Denial of Service) nth-check Dependency in Jira Software / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-42342 DoS (Denial of Service) react-router Dependency in Jira Software / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-34077 XSS (Cross Site Scripting) turbo-stream Dependency in Jira Software / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2026-42587 DoS (Denial of Service) netty-codec / netty-codec-http2 Dependency in Jira Software / Jira Service Management Data Center (CVSS: 7.5)
- CVE-2019-11272 BASM (Broken Authentication & Session Management) Spring Security Core Dependency in Fisheye/Crucible (CVSS: 7.3)

- CVE-2025-22228 BASM (Broken Authentication & Session Management) Spring Security Core Dependency in Fisheye/Crucible (CVSS: 7.4)
- CVE-2024-22257 Improper Authorization Spring Security Core Dependency in Fisheye/Crucible (CVSS: 8.2)

**Fixed Versions**

**Bamboo Data Center and Server**

- 12.1.8 (LTS) – Data Center only (recommended)
- 10.2.20 (LTS) – Data Center only

**Bitbucket Data Center and Server**

- 10.3.1 – Data Center only
- 10.2.4 (LTS) – Data Center only (recommended)
- 9.4.21 (LTS) – Data Center only

**Confluence Data Center and Server**

- 10.2.13 (LTS) – Data Center only
- 9.2.21 (LTS) – Data Center only

**Crowd Data Center and Server**

- 7.2.1 – Data Center only (recommended)

**Jira Data Center and Server**

- 11.3.7 (LTS) – Data Center only (recommended)
- 10.3.22 (LTS) – Data Center only

**Jira Service Management Data Center and Server**

- 11.3.7 (LTS) – Data Center only (recommended)
- 10.3.22 (LTS) – Data Center only

## 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-june-16-2026-1796309326.html