مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Atlassian

Tracking #:432318999

Date:20-05-2026

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 May 2026 Security Bulletin addressing multiple vulnerabilities affecting several Atlassian Data Center and Server products, including Atlassian Bamboo, Bitbucket, Confluence, Fisheye/Crucible, Jira Software, and Jira Service Management. The bulletin includes multiple critical- and high-severity vulnerabilities that could allow remote code execution, denial of service, file inclusion, cross-site scripting, authentication issues, information disclosure, and security misconfiguration attacks.

Vulnerability Details

Critical Severity Vulnerabilities:

- **CVE-2026-29145** – Broken Authentication and Session Management
- **CVE-2026-22732** – Security Headers Omission

High Severity Vulnerabilities:

- **CVE-2026-5598** – Covert Timing Channel (Bouncy Castle dependency)
- **CVE-2026-27727** – Remote Code Execution (mchange-commons-java dependency)
- **CVE-2025-67030** – Directory Traversal (plexus-utils dependency)
- **CVE-2026-29062** – Denial of Service (multiple products)
- **CVE-2026-34487** – Information Disclosure (Tomcat dependency)
- **CVE-2026-34483** – Injection / Improper Encoding (Tomcat dependency)
- **CVE-2026-29129** – Security Misconfiguration (Tomcat dependency)
- **CVE-2026-39304** – Denial of Service (ActiveMQ dependency)
- **CVE-2026-33750** – Denial of Service (multiple products)
- **CVE-2024-45801** – Cross-Site Scripting (DOMPurify dependency)
- **CVE-2026-29146** – Information Disclosure (Confluence)
- **CVE-2026-24880** – HTTP Request/Response Smuggling (Tomcat dependency)
- **CVE-2026-24734** – Injection (Confluence)
- **CVE-2026-27830** – Remote Code Execution (c3p0 dependency)
- **CVE-2025-52999** – Remote Code Execution (jackson-core dependency)
- **CVE-2026-42198** – Denial of Service (PostgreSQL dependency)
- **CVE-2023-24998** – Denial of Service (commons-fileupload dependency)
- **CVE-2026-31802** – File Inclusion (Jira products)
- **CVE-2026-29786** – File Inclusion (Jira products)
- **CVE-2026-22029** – DOM-based XSS (Jira products)
- **CVE-2026-25639** – Denial of Service (Jira products)
- **CVE-2026-26960** – File Inclusion (Jira Service Management)

Fixed Versions

- **Bamboo Data Center and Server** – 12.1.7 (LTS), 10.2.19 (LTS), 9.6.26 (LTS)
- **Bitbucket Data Center and Server** – 10.2.2 to 10.2.3 (LTS), 9.4.19 to 9.4.20 (LTS)
- **Confluence Data Center and Server** – 10.2.11 (LTS), 9.2.20 (LTS)
- **Fisheye/Crucible** – 4.9.10
- **Jira Software Data Center and Server** – 11.3.5 to 11.3.6 (LTS), 10.3.20 to 10.3.21 (LTS), 9.12.35 (LTS)

- **Jira Service Management Data Center and Server** – 11.3.5 to 11.3.6 (LTS), 10.3.20 to 10.3.21 (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-may-19-2026-1786839142.html