مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Atlassian July 2026 Security Bulletin

Tracking #:432319323

Date:22-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Atlassian has released its July 2026 Security Bulletin, addressing 101 third-party dependency vulnerabilities, including 18 Critical and 83 High severity issues affecting multiple Atlassian Data Center and Server products.

TECHNICAL DETAILS:

Atlassian has released its July 2026 Security Bulletin, addressing 101 third-party dependency vulnerabilities, including 18 Critical and 83 High severity issues affecting multiple Atlassian Data Center and Server products. The vulnerabilities primarily originate from third-party libraries such as Axios, Netty, Lodash, Apache ActiveMQ, Apache Tomcat, Bouncy Castle, Immutable.js, Fast-URI, and others integrated into Atlassian products.

Although Atlassian has assessed these vulnerabilities as presenting a lower practical risk in the context of their products, many of the vulnerabilities carry CVSS scores between 9.1 and 10.0 and include impacts such as Remote Code Execution (RCE), Server-Side Request Forgery (SSRF), HTTP Request Smuggling, Prototype Pollution, Authentication Bypass, Information Disclosure, File Inclusion, Injection, and Denial of Service (DoS).

Organizations using Jira Software, Jira Service Management, Confluence, Bitbucket, Bamboo, Crowd, Fisheye/Crucible, and Sourcetree should review affected versions and upgrade to the latest fixed releases as soon as possible.

Vulnerability Details:

Bamboo Data Center

- **CVE-2026-4800 – Remote Code Execution (Lodash Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2026-45505 – Remote Code Execution (Apache ActiveMQ Dependency)**
  CVSS: 8.8 (High)
- **CVE-2026-44494 – Injection (Axios Dependency)**
  CVSS: 8.7 (High)
- **CVE-2026-44490 – Injection (Axios Dependency)**
  CVSS: 8.2 (High)
- **CVE-2026-42588 – Remote Code Execution (Apache ActiveMQ Dependency)**
  CVSS: 8.1 (High)
- **CVE-2026-44249 – Improper Authorization (Netty Dependency)**
  CVSS: 8.1 (High)
- **CVE-2026-29146 – Information Disclosure (Apache Tomcat Dependency)**
  CVSS: 7.5 (High)
- **CVE-2026-45416 – Denial of Service (Netty Handler Dependency)**
  CVSS: 7.5 (High)
- **CVE-2026-50010 – Improper Verification of Cryptographic Signature (Netty Handler)**
  CVSS: 7.5 (High)
- **CVE-2026-44495 – Remote Code Execution (Axios Dependency)**
  CVSS: 7.0 (High)

Bitbucket Data Center

- **CVE-2020-28282 – Remote Code Execution (getobject Dependency)**
  CVSS: 9.8 (Critical)

- **CVE-2026-5598 – Cryptographic Failure (Bouncy Castle Dependency)**
  CVSS: 8.9 (High)
- **CVE-2026-33871 – Denial of Service (Netty Dependency)**
  CVSS: 8.7 (High)
- **CVE-2026-44494 – Injection**
  CVSS: 8.7 (High)
- **CVE-2026-35554 – Race Condition**
  CVSS: 8.7 (High)
- **CVE-2026-44492 – Server-Side Request Forgery (SSRF)**
  CVSS: 8.6 (High)
- **CVE-2026-42041 – Injection (Axios Dependency)**
  CVSS: 8.2 (High)
- **CVE-2026-44490 – Injection**
  CVSS: 8.2 (High)
- **CVE-2026-22731 – Broken Authentication & Session Management**
  CVSS: 8.2 (High)
- **CVE-2026-44487 – Information Disclosure**
  CVSS: 8.2 (High)

Confluence Data Center

- **CVE-2026-42043 – Server-Side Request Forgery (Axios Dependency)**
  CVSS: 10.0 (Critical)
- **CVE-2025-62718 – Server-Side Request Forgery (Axios Dependency)**
  CVSS: 9.9 (Critical)
- **CVE-2026-4800 – Remote Code Execution (Lodash Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2026-2332 – HTTP Request Smuggling (Jetty Dependency)**
  CVSS: 9.1 (Critical)
- **CVE-2026-42264 – Prototype Pollution (Axios Dependency)**
  CVSS: 9.1 (Critical)
- **CVE-2026-40175 – Server-Side Request Forgery (Axios Dependency)**
  CVSS: 9.0 (Critical)
- **CVE-2026-44494 – Injection (Axios Dependency)**
  CVSS: 8.7 (High)
- **CVE-2026-12143 – Remote Code Execution (Form-Data Dependency)**
  CVSS: 8.7 (High)
- **CVE-2026-44492 – Server-Side Request Forgery (Axios Dependency)**
  CVSS: 8.6 (High)
- **CVE-2026-31802 – File Inclusion (Node-Tar Dependency)**
  CVSS: 8.2 (High)

Jira Software

- **CVE-2022-37601 – Prototype Pollution (parseQuery Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2026-42581 – HTTP Request Smuggling (Netty Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2025-14813 – Cryptographic Failure (Bouncy Castle Dependency)**
  CVSS: 9.3 (Critical)
- **CVE-2026-29145 – Broken Authentication & Session Management**
  CVSS: 9.1 (Critical)

- **CVE-2026-42044 – Prototype Pollution (Axios Gadget)**
  CVSS: 9.1 (Critical)

Jira Service Management

- **CVE-2022-37601 – Prototype Pollution (parseQuery Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2026-42581 – HTTP Request Smuggling (Netty Dependency)**
  CVSS: 9.8 (Critical)
- **CVE-2025-14813 – Cryptographic Failure (Bouncy Castle Dependency)**
  CVSS: 9.3 (Critical)
- **CVE-2026-29145 – Broken Authentication & Session Management**
  CVSS: 9.1 (Critical)
- **CVE-2026-42044 – Prototype Pollution (Axios Gadget)**
  CVSS: 9.1 (Critical)

Crowd Data Center

- **CVE-2026-27830 – Remote Code Execution (c3p0 Dependency)**
  CVSS: 8.9 (High)

Fisheye/Crucible

- **CVE-2024-7254 – Remote Code Execution (protobuf-java Dependency)**
  CVSS: 8.7 (High)
- **CVE-2022-3510 – Denial of Service (protobuf-java Dependency)**
  CVSS: 7.5 (High)
- **CVE-2022-3509 – Denial of Service (protobuf-java Dependency)**
  CVSS: 7.5 (High)
- **CVE-2021-22569 – Denial of Service (protobuf-java Dependency)**
  CVSS: 7.5 (High)

Sourcetree (Windows and Mac)

- **CVE-2026-21575 – Remote Code Execution**
  CVSS: 7.1 (High)

RECOMMENDATIONS:

Immediate Actions:

- Upgrade all affected Atlassian products to the latest fixed or Long-Term Support (LTS) versions recommended by Atlassian.
- Prioritize remediation of products affected by Critical vulnerabilities.
- Review internet-facing Atlassian deployments and restrict external access where possible.

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-21-2026-1821999345.html