مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Atlassian

Tracking #:432318415

Date:18-02-2026

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 INTELLGIENCE 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 that Atlassian has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Atlassian has released its February 2026 security updates addressing multiple critical and high-severity vulnerabilities affecting Bamboo, Confluence, and Crowd for Data Center and Server deployments.
Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, gain unauthorized access, disrupt services, or manipulate sensitive data within Atlassian applications, potentially compromising both server integrity and user data.

Vulnerability Details
Critical Severity

- **CVE-2025-66516** – XXE vulnerability in Apache Tika (Crowd) – CVSS 9.8
- **CVE-2025-9288** – Injection in sha.js (Crowd) – CVSS 9.1
- **CVE-2025-9287** – Injection in cipher-base (Crowd) – CVSS 9.1

High Severity

- **CVE-2025-66021** – DOM-based XSS in owasp-java-html-sanitizer (Bamboo) – CVSS 8.6
- **CVE-2025-59343** – File Inclusion in tar-fs (Confluence) – CVSS 8.7
- **CVE-2025-41249** – Improper Authorization in Spring Core (Confluence) – CVSS 7.5
- **CVE-2022-25883** – DoS in Confluence – CVSS 7.5
- **CVE-2020-28469** – DoS in Confluence – CVSS 7.5
- **CVE-2025-48976** – DoS in Confluence – CVSS 7.5
- **CVE-2022-25927** – DoS in Confluence – CVSS 7.5
- **CVE-2025-48734** – Remote Code Execution in commons-beanutils (Crowd) – CVSS 8.8
- **CVE-2025-66675** – DoS in struts2-core (Crowd) – CVSS 8.2
- **CVE-2019-20149** – Insecure Deserialization in kind-of dependency (Crowd) – CVSS 7.5
- **CVE-2024-57699** – DoS in third-party dependency (Crowd) – CVSS 7.5

Fixed Versions
Bamboo Data Center and Server

- 12.1.2 (LTS) – recommended Data Center only
- 10.2.14 to 10.2.15 (LTS) – Data Center only

Confluence Data Center and Server

- 10.2.6 (LTS) – recommended Data Center only
- 10.2.3 (LTS) – Data Center only
- 9.2.15 (LTS) – Data Center only
- 9.2.14 (LTS) – Data Center only

Crowd Data Center and Server

- 7.1.4 – recommended 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-february-17-2026-1722256046.html