



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - Atlassian
Tracking #:432316988
Date:19-03-2025

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

TECHNICAL DETAILS:

Atlassian has released its March 2025 Security Bulletin, addressing 13 high-severity vulnerabilities across various products, including Bamboo, Bitbucket, Crowd, Jira Software, and Jira Service Management (Data Center and Server). Successful exploitation of these vulnerabilities could lead to denial of service, unauthorized data access, arbitrary code execution, and potential compromise of sensitive information.

Affected Products and Vulnerabilities:

1. Bamboo Data Center and Server

- Vulnerabilities: Denial of Service (DoS) in io.netty:netty-handler dependency.
- CVE ID: CVE-2025-24970 (CVSS Score: 7.5 High).
- Fixed Versions: 10.2.2 (LTS), 9.6.11 (LTS).

2. Bitbucket Data Center and Server

- Vulnerabilities:
 - Third-party dependencies (CVE-2024-4367, CVE-2024-45296).
 - Denial of Service (DoS) in org.bouncycastle:bcprov-jdk18on dependency (CVE-2024-29857).
 - SQL Injection in org.postgresql:postgresql dependency (CVE-2022-31197, CVE-2022-21724).
- CVSS Scores: Range from 7.0 to 8.8 High.
- Fixed Versions: 9.5.1–9.5.2, 8.19.15–8.19.16 (LTS), 9.4.3–9.4.4 (LTS), 8.9.25 to 8.9.26 (LTS)

3. Crowd Data Center and Server

- Vulnerabilities:
 - Denial of Service (DoS) in com.nimbusds:nimbus-jose-jwt, io.netty:netty-handler, and io.netty:netty-codec-http2 dependencies.
- CVE IDs: CVE-2023-52428, CVE-2025-24970, CVE-2023-44487 (CVSS Scores: 7.5 High).
- Fixed Version: 6.2.0 to 6.2.2.

4. Jira Data Center and Server

- Vulnerabilities:
 - Path Traversal in org.springframework:spring-webmvc dependency (CVE-2024-38819).
 - DoS in com.thoughtworks.xstream:xstream dependency (CVE-2024-47072).
- CVSS Score: 7.5 High.
- Fixed Versions: 10.5.0, 10.3.4 (LTS), 9.12.19 (LTS).

5. Jira Service Management Data Center and Server

- Vulnerabilities:
 - Path Traversal in org.springframework:spring-webmvc dependency (CVE-2024-38819).
 - DoS in com.thoughtworks.xstream:xstream dependency (CVE-2024-47072).
- CVSS Score: 7.5 High.
- Fixed Versions: 10.5.0, 10.3.4 (LTS), 5.12.19 (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-march-18-2025-1527943363.html>