مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Atlassian

Tracking #:432317638

Date:26-08-2025

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 security updates addressing 15 vulnerabilities across Bamboo, Bitbucket, and Crowd Data Center and Server, including 14 high-severity and 1 critical-severity issue. The vulnerabilities can lead to denial of service (DoS), security misconfigurations, and potential exposure of sensitive administrative functions.

Affected Products and Vulnerabilities

Bamboo Data Center and Server

- **Vulnerabilities:**
  - CVE-2025-53506 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-52520 – DoS via Third-Party Dependency – CVSS 7.5 High
- **Affected Versions:** 11.0.0 – 11.0.3, 10.2.0 – 10.2.6 (LTS), 9.6.0 – 9.6.15 (LTS)
- **Fixed Versions:** 11.0.4 (Data Center only), 10.2.7 (LTS, Data Center only), 9.6.16 (LTS, Data Center only)

Bitbucket Data Center and Server

- **Vulnerabilities:**
  - CVE-2025-49146 – Security Misconfiguration – CVSS 8.2 High
  - CVE-2025-49125 – Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-48988 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-53506 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-52520 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-52434 – DoS via Third-Party Dependency – CVSS 7.5 High
- **Affected Versions:** 9.6.0 – 9.6.4, 9.5.0 – 9.5.2, 9.4.0 – 9.4.8 (LTS), 9.3.0 – 9.3.2, 9.2.0 – 9.2.1, 8.19.0 – 8.19.20 (LTS)
- **Fixed Versions:** 9.6.5 (DC only), 9.4.9 (LTS, DC only), 8.19.21 (LTS, DC only)

Crowd Data Center and Server

- **Vulnerabilities:**
  - CVE-2025-7783 – Third-Party Dependency (Critical) – CVSS 9.4 Critical
  - CVE-2025-48976 – DoS in Crowd Data Center – CVSS 8.7 High
  - CVE-2025-48976 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-52434 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-53506 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-52520 – DoS via Third-Party Dependency – CVSS 7.5 High
  - CVE-2025-48988 – DoS via Third-Party Dependency – CVSS 7.5 High
- **Affected Versions:** 6.3.0 – 6.3.1, 6.2.0 – 6.2.4, 6.1.0 – 6.1.6, 6.0.0 – 6.0.10, 5.3.0 – 5.3.7
- **Fixed Versions:** 6.3.2 (DC only), 6.2.5 (DC only), 5.3.8 (DC 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-august-19-2025-1621491738.html