مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Atlassian

Tracking #:432318631

Date:20-03-2026

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 March 2026 Security Bulletin addressing multiple high-severity vulnerabilities across various products. These issues may allow attackers to perform remote code execution (RCE), path traversal, file inclusion, denial of service (DoS), and cross-site scripting (XSS), potentially leading to system compromise or service disruption.

Vulnerability Details
Bamboo Data Center & Server

- **CVE-2026-21570** – Remote Code Execution (RCE) – CVSS 8.6
- **CVE-2025-68493** – Missing XML Validation (Apache Struts) – CVSS 8.1
- **CVE-2025-64775** – Denial of Service (Apache Struts) – CVSS 7.1

Bitbucket Data Center & Server

- **CVE-2022-25883** – Denial of Service (semver dependency) – CVSS 7.5

Confluence Data Center & Server

- **CVE-2025-64756** – OS Command Injection (glob dependency) – CVSS 7.5

Crowd Data Center & Server

- **CVE-2026-21884** – DOM-based Cross-Site Scripting (react-router-dom) – CVSS 8.2
- **CVE-2026-22029** – DOM-based Cross-Site Scripting (@remix-run/router) – CVSS 8.0
- **CVE-2026-25639** – Denial of Service (axios dependency) – CVSS 7.5

Fisheye / Crucible

- **CVE-2023-52428** – Denial of Service (nimbus-jose-jwt dependency) – CVSS 7.5

Jira Software Data Center & Server

- **CVE-2026-23950** – Path Traversal (node-tar dependency) – CVSS 8.8
- **CVE-2026-23745** – File Inclusion (node-tar dependency) – CVSS 8.2
- **CVE-2026-24842** – File Inclusion (node-tar dependency) – CVSS 8.2
- **CVE-2022-25927** – Denial of Service (ua-parser-js dependency) – CVSS 7.5
- **CVE-2022-25883** – Denial of Service (semver dependency) – CVSS 7.5
- **CVE-2020-28469** – Denial of Service (glob-parent dependency) – CVSS 7.5

Jira Service Management Data Center & Server

- **CVE-2026-23950** – Path Traversal (node-tar dependency) – CVSS 8.8
- **CVE-2026-23745** – File Inclusion (node-tar dependency) – CVSS 8.2
- **CVE-2026-24842** – File Inclusion (node-tar dependency) – CVSS 8.2
- **CVE-2024-57699** – Denial of Service (json-smart dependency) – CVSS 7.5
- **CVE-2022-25927** – Denial of Service (ua-parser-js dependency) – CVSS 7.5
- **CVE-2020-28469** – Denial of Service (glob-parent dependency) – CVSS 7.5

Fixed Versions

- **Bamboo Data Center & Server:** 12.1.3 (LTS), 10.2.16 (LTS), 9.6.24 (LTS)
- **Bitbucket Data Center & Server:** 10.2.0–10.2.1 (LTS), 10.1.5, 9.4.17–9.4.18 (LTS)
- **Confluence Data Center & Server:** 10.2.7 (LTS), 9.2.15–9.2.17 (LTS), 9.0.2–9.0.3
- **Crowd Data Center & Server:** 7.1.5, 6.3.5
- **Fisheye / Crucible:** 4.9.8

- **Jira Software Data Center & Server:** 11.3.3 (LTS), 10.3.18 (LTS)
- **Jira Service Management Data Center & Server:** 11.3.3 (LTS), 10.3.18 (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-17-2026-1721271371.html