مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Atlassian Products

Tracking #:432317292

Date:21-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Atlassian has released its May 2025 Security Bulletin, disclosing multiple high-severity vulnerabilities across multiple Atlassian products, including Bamboo, Confluence, Jira Software, Jira Service Management, and Fisheye/Crucible.

TECHNICAL DETAILS:

Atlassian has released its May 2025 Security Bulletin, disclosing multiple high-severity vulnerabilities across multiple Atlassian products, including Bamboo, Confluence, Jira Software, Jira Service Management, and Fisheye/Crucible.

These vulnerabilities, discovered through Atlassian's Bug Bounty program and security testing, primarily relate to Denial of Service (DoS) risks through third-party dependencies and Privilege Escalation flaws within Jira components.

All organizations using affected versions should prioritize patching immediately to mitigate risks of service disruption and unauthorized privilege elevation.

Vulnerability Details:

CVE ID	Description	Severity	Affected Products
CVE-2025-31650	DoS via org.apache.tomcat:tomcat-coyote	7.5 (High)	Bamboo, Confluence
CVE-2024-47072	DoS via com.thoughtworks.xstream:xstream	7.5 (High)	Confluence
CVE-2024-57699	DoS via net.minidev:json-smart	7.5 (High)	Fisheye/Crucible
CVE-2025-24970	DoS via io.netty:netty-handler	7.5 (High)	Jira Software, Jira Service Management
CVE-2025-22157	Privilege Escalation in Jira products	7.2 (High)	Jira Software, Jira Service Management

Fixed Versions:

Product	Recommended Fixed Version
Bamboo	11.0.1 (DC), 10.2.4 (LTS), 9.6.13 (LTS)
Confluence	9.4.1 (DC), 9.2.4 (LTS), 8.5.22 (LTS)
Fisheye/Crucible	4.9.1
Jira Software	10.6.0 (DC), 10.3.6 (LTS), 9.12.23 (LTS)
Jira Service Management	10.6.0 (DC), 10.3.6 (LTS), 5.12.23 (LTS)

RECOMMENDATIONS:

- Patch Immediately: Upgrade to the latest fixed version for the affected products.
- Prioritize High-Risk Environments: Focus on production systems and environments with external exposure first.
- Monitor Exploitation: Monitor application and infrastructure logs for unusual activity. Consider implementing WAF rules to block known vectors where patching is delayed.

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-may-20-2025-1561365992.html