



CERT-In Advisory CIAD-2025-0040

Multiple Vulnerabilities in Atlassian Products

Original Issue Date: October 28, 2025

Severity Rating: High

Software Affected

- Bamboo Data Center and Server
- Fisheye/Crucible
- Jira Data Center and Server
- Jira Service Management Data Center and Server

Overview

Multiple vulnerabilities have been reported in Atlassian Products which could allow an attacker to perform Path Traversal (Arbitrary Write), HTTP Request Smuggling, SMTP Injection or cause DoS (Denial of Service) conditions on the targeted system.

Target Audience:

Individuals and organisational users of the above mentioned Atlassian products.

Risk Assessment:

High risk of sensitive information disclosure, resource exhaustion or session hijacking.

Impact Assessment:

Potential for unauthorized access, service disruption or system compromise.

Description

Atlassian products are used by software development teams, IT operations, project management professionals and business teams. Some of the products in the Atlassian suite include Jira, Fisheye and Bamboo.

Multiple vulnerabilities have been reported in various Atlassian Products; Details of which are provided below:

Affected Products	Affected Versions	Severity	Impact	CVE ID
Bamboo Data Center and Server	11.0.0 to 11.0.4 10.2.0 to 10.2.7 (LTS) 9.6.0 to 9.6.16 (LTS)	High	DoS (Denial of Service)	CVE-2025-48989
Fisheye/Crucible	4.9.0 to 4.9.2 4.8.14 to 4.8.16	High	DoS (Denial of Service)	CVE-2025-48976
Jira Data Center and Server	11.0.0 to 11.0.1 10.7.1 to 10.7.4 10.6.0 to 10.6.1 10.5.0 to 10.5.1 10.4.0 to 10.4.1 10.3.0 to 10.3.11 (LTS) 10.2.0 to 10.2.1 10.1.1 to 10.1.2 10.0.0 to 10.0.1 9.17.0 to 9.17.5 9.16.0 to 9.16.1 9.15.2 9.14.0 to 9.14.1 9.13.0 to 9.13.1 9.12.0 to 9.12.27 (LTS)	High	Path Traversal (Arbitrary Write) HTTP Request Smuggling DoS (Denial of Service) SMTP Injection	CVE-2025-22167 CVE-2025-58057 CVE-2025-58056 CVE-2025-48989 CVE-2025-7962
Jira Service Management Data Center and Server	11.0.0 to 11.0.1 10.7.1 to 10.7.4 10.6.0 to 10.6.1 10.5.0 to 10.5.1 10.4.0 to 10.4.1 10.3.0 to 10.3.11 (LTS) 10.2.0 to 10.2.1 10.1.1 to 10.1.2 10.0.0 to 10.0.1 5.17.0 to 5.17.5 5.16.0 to 5.16.1 5.15.2 5.14.0 to 5.14.1 5.13.0 to 5.13.1 5.12.0 to 5.12.27 (LTS)	High	Path Traversal (Arbitrary Write) HTTP Request Smuggling DoS (Denial of Service) SMTP Injection	CVE-2025-22167 CVE-2025-58057 CVE-2025-58056 CVE-2025-48989 CVE-2025-7962

Solution

Apply appropriate updates as mentioned in Atlassian security bulletin:

<https://confluence.atlassian.com/security/security-bulletin-october-21-2025-1652920034.html>

Vendor Information

Atlassian

<https://confluence.atlassian.com/security/security-bulletin-october-21-2025-1652920034.html>

References

Atlassian

<https://confluence.atlassian.com/security/security-bulletin-october-21-2025-1652920034.html>

CVE Name

[CVE-2025-48989](#)

[CVE-2025-48976](#)

[CVE-2025-22167](#)

[CVE-2025-58057](#)

[CVE-2025-58056](#)

[CVE-2025-7962](#)

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in

Phone: +91-11-22902657

Postal address

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics and Information Technology

Government of India

Electronics Niketan

6, CGO Complex, Lodhi Road,

New Delhi - 110 003

India

