Two Vulnerabilities in The Atlassian Jira Server and Data Center

Vairav Advisory Report

Date: February 10, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

EXECUTIVE SUMMARY

CVE-2019-11581 and CVE-2021-26086 were previously disclosed in the Atlassian Jira Server and Data Center but have been recently updated. CVE-2019-11581 is a server-side template injection vulnerability that allows remote code execution (RCE) on affected systems, while CVE-2021-26086 is a path traversal vulnerability that enables unauthorized access to specific files. Organizations using vulnerable versions of Jira are strongly advised to upgrade immediately.

VULNERABILITY DETAILS

CVE-2019-11581

Description: A server-side template injection vulnerability allows an attacker to execute arbitrary code remotely. The issue exists in the ContactAdministrators and SendBulkMail actions.

Impact: Remote Code Execution (RCE), complete system compromise.

CVSS Score: 9.8 (Critical)

Affected Versions:

Jira Server & Data Center:

- 4.4.0 before 7.6.14
- 7.7.0 before 7.13.5
- 8.0.0 before 8.0.3
- 8.1.0 before 8.1.2
- 8.2.0 before 8.2.3

CVE-2021-26086

Description: A path traversal vulnerability allows unauthorized access to specific files via the /WEB-INF/web.xml endpoint.

Impact: Information disclosure, and unauthorized file access.

CVSS Score: 5.3 (Medium)

Affected Versions:

Jira Server & Data Center:

- Before version 8.5.14
- 8.6.0 before 8.13.6

- 8.14.0 before 8.16.1

EXPLOIT DETAILS

Attackers can exploit CVE-2019-11581 to gain full system control by sending maliciously crafted requests. CVE-2021-26086 can be exploited to read sensitive files, leading to information disclosure risks.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Atlassian has released patches to mitigate these vulnerabilities. Users should upgrade to the latest supported versions of Jira Server and Data Center.

ADDITIONAL SECURITY MEASURES

- Restrict access to sensitive Jira endpoints and configure appropriate user permissions.
- Disable unnecessary features and enforce security best practices.

REFERENCES

https://app.opencve.io/cve/CVE-2019-11581

https://app.opencve.io/cve/CVE-2021-26086

https://nvd.nist.gov/vuln/detail/CVE-2019-11581

https://nvd.nist.gov/vuln/detail/CVE-2021-26086

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com