GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 October 2026

Advisory 359: Atlassian Data Center Path Traversal Arbitrary File Access Vulnerability in Multiple Products - Actively Exploited (CVE-2026-21589).

Release Date: 15th October 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-21589 is a path traversal vulnerability (arbitrary file access) in eight self-managed Atlassian products. An unauthenticated attacker with network access can read specific files inside the web application root directory by sending a crafted request. The attacker must already know the exact file name and path, and cannot list directories

The flaw does not give code execution directly, but exposed configuration files can lead to a full compromise. watchTowr showed that where Jira is integrated with Crowd, an attacker can read crowd.properties, which stores the Crowd application credentials in plaintext, and use them to create a user and add it to the jira-administrators group. Crowd IP allowlisting can block this path. Atlassian Cloud has already been patched and Cloud customers need no action.

What are the systems affected?

The following self-managed Atlassian products are affected. All versions before the fixed releases are vulnerable:

- Bitbucket Data Center

- Confluence Data Center
- Jira Software Data Center
- Jira Service Management Data Center
- Bamboo Data Center
- Crowd Data Center
- Crucible
- Fisheye

Not affected / patched version:

- Bitbucket Data Center 9.4.26, 10.2.8 or 10.5.1
- Confluence Data Center 9.2.26 or 10.2.19
- Jira Software Data Center 9.12.40, 10.3.26 or 11.3.12
- Jira Service Management Data Center 5.12.40, 10.3.26 or 11.3.12
- Bamboo Data Center 10.2.24 or 12.1.12
- Crowd Data Center 6.3.7, 7.0.3, 7.1.7 or 7.2.4
- Crucible and Fisheye 4.9.15
- Atlassian Cloud products are already patched

What does this mean?

Successful exploitation may allow attackers to:

- Read configuration files and secrets stored in the web application root without logging in
- Steal credentials, for example the plaintext Crowd application password in crowd.properties, and use them to create administrator accounts in Jira
- Use the compromised Atlassian server, which holds source code, tickets and build pipelines, as a foothold into the network

Mitigation process

CERTVU recommends the following:

1. Patch to the fixed release
Upgrade each self-managed instance to a fixed version for its branch, starting with internet-facing instances. This is the permanent fix.

2. Apply temporary mitigations if patching is delayed
Take the instance off the public internet, or apply a WAF or reverse proxy rule blocking path traversal sequences including URL-encoded variants. Atlassian also provides a Tomcat RewriteValve workaround for Confluence, Jira, Bamboo and Crowd, and a urlrewrite.xml rule for Bitbucket. Back up before applying these. They reduce the risk but do not replace patching.

3. Hunt for compromise

Report suspected compromise to CERTVU.

Reference

1. https://www.atlassian.com/trust/security/advisories
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

3. https://www.infosecurity-magazine.com/news/critical-vulnerability-atlassian/
4. https://securityweek.com/attackers-target-critical-atlassian-vulnerability-within-hours-of-poc-publication
5. https://senserva.com/cve/CVE-2026-21589.html
6. https://nvd.nist.gov/vuln/detail/CVE-2026-21589