Atlassian file read

CREDENTIAL AND IDENTITY REVIEW / CVE-2026-21589 / OCTOBER 16, 2026

01 Scope, protect, and preserve

For affected self-hosted Atlassian products. The administrator-creation example is a conditional Jira + Crowd chain; use the sections relevant to your deployment.

Case / investigation reference

Review owner

Review date

Product

Version / release branch

Instance / node inventory reference

Exposure window: start

Exposure window: end

Time zone / clock differences

Mitigation / patch applied

Applied at: date, time, and zone

IDENTIFY THE EXPOSURE

- [ ] Record the product, release branch, owner, and affected instances or cluster nodes.
- [ ] Establish when the vulnerable instance was reachable and through which access path.
- [ ] Include mirrors and additional nodes covered by the vendor guidance.
- [ ] Identify sensitive files actually present inside the web application root.

PROTECT AND PRESERVE

- [ ] Apply the supported fix or the vendor's temporary mitigation; record when it took effect.
- [ ] Retain available proxy, HTTP access, application, Crowd, and identity records.
- [ ] Preserve response outcomes and content where available, with timestamps and clock offsets.

> Do not delay urgent protection to collect evidence. A matching request or HTTP 200 alone does not establish that a sensitive file was returned.

Follow the application identity

CREDENTIAL AUTHORITY / API ACTIVITY / ACCOUNT CHANGES

02 Check what the credential can do

The demonstrated Jira + Crowd chain depends on three conditions. Review the actual application configuration and retained records.

REACHABILITY	SOURCE RESTRICTIONS	DIRECTORY AUTHORITY
Crowd can be reached	The source is accepted	The actions are permitted

Crowd application identity

Mapped directories / configuration reference

Allowed source addresses / policy reference

User / group permissions or configuration reference

REVIEW THE APPLICATION CREDENTIAL

- [ ] If the application secret was exposed or could have been returned, rotate it through the supported workflow and update dependent configurations.
- [ ] Record mapped directories, allowed sources, and user/group write permissions.
- [ ] Separate attempted API access, accepted access, and completed changes.

ACCOUNT FOR CHANGES

- [ ] Review users created during the exposure window and the identity responsible.
- [ ] Review administrator-group changes and reconcile them with approved administration.
- [ ] For unauthorized changes, contain resulting access and investigate later sessions and actions.

Identity findings / supporting record references

Record credential identifiers and evidence references, not secret values. Rotation does not remove an account created earlier.

Record the evidence and next steps

FINDINGS / COVERAGE / ACCOUNTABLE FOLLOW-UP

03 Keep each evidence state separate

Choose a finding and cite the record that supports it. "Not found" applies only to the reviewed records and their coverage.

File-read request observed

Not reviewed

Evidence / record reference

Sensitive file exposure

Not reviewed

Evidence / record reference

Application credential use

Not reviewed

Evidence / record reference

Unauthorized identity change

Not reviewed

Evidence / record reference

Log coverage gaps / retention limits / unresolved questions

Next action / containment or investigation follow-up

Action owner

Follow-up date

SOURCE REFERENCES

Atlassian advisory and fixed releases

Crowd directory permissions

Use retained records and authorized configuration review. This worksheet does not require exploit requests.