CHECKLIST · SCAMS & SECURITY

Atlassian's critical file-access flaw needs an urgent check with your IT provider

Published 7 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/atlassian-data-center-file-access-october-2026/

- [ ] **Confirm the deployment today.** Ask your IT provider whether each Atlassian service is Atlassian Cloud or a self-managed installation.
- [ ] **Record the installed versions.** Have the administrator match each affected product to the official CVE-2026-21589 fixed-version table.
- [ ] **Agree the work window.** Get a named owner, expected interruption and completion time from the provider; ask about temporary protection if patching must wait.
- [ ] **Save the completion record.** Request the resulting versions and confirmation of which installations were covered in the support ticket.
- [ ] **Assign the exposure check.** Ask who will review affected instances using Atlassian's detection guidance and report the findings to the business.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.