# CERT-EU: Critical file access flaw (CVE-2026-21589) in Atlassian Data Center products



Atlassian disclosed CVE-2026-21589 (CVSS 9.3), letting unauthenticated attackers read specific files on several Data Center products. CERT-EU urges upgrading, internet-facing instances first, and checking access logs.

- CVE-2026-21589 has a CVSS score of 9.3 and allows unauthenticated access to specific files in the web application root directory.
- Affected: Bitbucket, Confluence, Jira Service Management, Jira Software, Bamboo and Crowd Data Center, plus Crucible and Fisheye.
- Attackers must know the exact file name and path; directory listing is not possible.
- Atlassian says Cloud products are already patched and it has found no evidence of exploitation.
- CERT-EU advises upgrading internet-facing instances first and reviewing access logs for

> compromise.

On 5 October 2026, Atlassian published an advisory on a critical arbitrary file access vulnerability, tracked as **CVE-2026-21589** with a CVSS score of 9.3. CERT-EU republished the guidance as advisory 2026-015.

## What the flaw allows

An unauthenticated attacker can reach specific files inside the web application root directory. Exploitation requires knowing the exact name and path of the target file, and the flaw does not let an attacker list directory contents. Atlassian notes that some configurations may hold sensitive files, which raises the risk.

All versions earlier than the fixed releases are affected across Bitbucket, Confluence, Jira Service Management, Jira Software, Bamboo and Crowd Data Center, as well as Crucible and Fisheye. Fixed versions are listed in the vendor advisory. Atlassian states that its Cloud products have been patched and that it has found no evidence of exploitation.

## Recommended handling

CERT-EU recommends upgrading to a fixed or the latest version as soon as possible, starting with internet-facing instances. Atlassian suggests moving to the fixed LTS version or later.

Where patching cannot happen immediately, the advisory offers these interim measures:

- Take the instance off the internet until it is patched, including instances that require user login.
- Apply a blocking rule on the web application firewall or proxy for path-traversal patterns, and test it, including URL-encoded forms.
- For most products, enable Tomcat's RewriteValve with a rewrite configuration; for Bitbucket, add a blocking rule to its URL rewrite file and restart. Back up first.

CERT-EU also recommends checking access logs for traversal patterns. If compromise is suspected, investigate the instance, review and rotate any exposed credentials or secrets, and contact the relevant cybersecurity authority. Exact configuration snippets are in Atlassian's advisory.

## What to do now

1. Inventory all Atlassian Data Center, Crucible and Fisheye instances and compare their versions with the fixed versions in Atlassian's advisory.
2. Upgrade affected instances to a fixed or the latest version, prioritising those reachable from the internet.
3. Where patching must wait, remove the instance from internet exposure or apply the WAF/proxy or product-level blocking rule from the advisory, after a backup, and test it.
4. Review access logs for path-traversal patterns, checking both URL-decoded and raw log lines.

5. If compromise is suspected, rotate potentially exposed credentials and secrets, investigate, and notify the National Cybersecurity Authority (NCA) and your sector regulator as applicable.