



Security Advisory 2026-015

Critical Vulnerability in Multiple Atlassian Products

2026-10-06 — v1.0

TLP:CLEAR

History:

- 06/10/2026 — v1.0 – Initial publication

Summary

On 5 October 2026, Atlassian published a security advisory addressing a **critical arbitrary file access** vulnerability. It affects **Bitbucket Data Center, Confluence Data Center, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center, Crowd Data Center, Crucible** and **Fisheye** [1].

CERT-EU strongly recommends upgrading all affected installations to a fixed version as soon as possible, starting with instances accessible from the internet. CERT-EU also recommends checking access logs for signs of exploitation.

Technical Details

The vulnerability **CVE-2026-21589**, with a CVSS score of 9.3, is an **arbitrary file access** vulnerability that allows an unauthenticated attacker to access specific files within the web application root directory [1].

To exploit the vulnerability, an attacker needs to know the target file's exact name and path in advance. The vulnerability does not allow attackers to enumerate or list directory contents. Atlassian notes that some configurations may contain sensitive files that increase the risk [1].

Affected Products

All versions earlier than the fixed versions listed below are affected [1]:

Product	Fixed Versions
Bitbucket Data Center	9.4.26, 10.2.8, 10.5.1
Confluence Data Center	9.2.26, 10.2.19
Jira Service Management Data Center	5.12.40, 10.3.26, 11.3.12
Jira Software Data Center	9.12.40, 10.3.26, 11.3.12
Bamboo Data Center	10.2.24, 12.1.12
Crowd Data Center	6.3.7, 7.0.3, 7.1.7, 7.2.4
Crucible	4.9.15

Product	Fixed Versions
Fisheye	4.9.15

Atlassian states that affected Atlassian Cloud products have been patched and that its investigation has not found evidence of exploitation [1].

Additional information is available in the vendor's advisory [1].

Recommendations

CERT-EU strongly recommends upgrading all affected installations to a fixed version or the latest version as soon as possible, starting with internet-facing instances. Atlassian recommends patching to the fixed LTS version or later [1]. CERT-EU also recommends checking access logs for signs of exploitation.

Mitigation

If patching is not immediately possible, **remove the instance from the internet until it can be patched or mitigated** (this includes instances accessible from the public internet that require user authentication) [1], or:

- **Option 1 (all affected products):** apply a rule on the Web Application Firewall or proxy layer that blocks any URL matching the regular expression below. Then test that the rule blocks `...` immediately adjacent to `/`, `\`, or `::`, including URL-encoded forms [1].

```
(?is).*?(?:/|\\|::|%(?:25)*(?:2f|5c)|(?:|%(?:25)*3a){2})(?:\.|%(?:25)*2e){2}(?:/|\\|::|%(?:25)*
(?:2f|5c)|(?:|%(?:25)*3a){2}|%(?:25)*3b|$).*
```

- **Option 2 (Confluence, Jira Service Management, Jira, Bamboo and Crowd):** on each node, enable Tomcat's RewriteValve in the application `<Context>` element and install a `rewrite.config` file in the `WEB-INF` directory to block such requests [1].
- **Option 3 (Bitbucket only):** add a blocking rule at the top of `./app/WEB-INF/urlrewrite.xml` on all nodes, mirrors and mirror farm nodes, then restart Bitbucket Data Center [1].

Back up the instance before applying Option 2 or Option 3. The exact configuration snippets are in the vendor's advisory [1].

Compromise assessment

CERT-EU recommends checking all affected instances for evidence of compromise. To investigate access logs, Atlassian suggests one of these approaches [1]:

- URL-decode each access-log request line, then check for `...` immediately adjacent to `/`, `\`, or `::` [1].
- Search raw (non-decoded) log lines directly with the regular expression shown above [1].

If a compromise is suspected, CERT-EU recommends investigating the affected instances, reviewing and rotating any credentials or secrets that may have been exposed, and contacting the relevant cybersecurity authority.

References

- [1] <https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html>