contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Atlassian Multiple Products exploited

CVE-2026-21589 · on CISA's exploited list since 15 October 2026

Analysis Report

If you run Atlassian Data Center products, act now: CISA's date of 18 October 2026 has passed. First find which of these products you run and whether any can be reached from the internet. If you run …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 9.3**	STATUS	On CISA's exploited list; due 18 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/atlassian-multiple-products-cve-2026-21589

The bottom line

> *If you run Atlassian Data Center products, act now: CISA's date of 18 October 2026 has passed. First find which of these products you run and whether any can be reached from the internet. If you run none, you can stop reading.*

At a glance

Fact	Detail
Product	Atlassian Multiple Products (CVE-2026-21589)
Severity	Critical: 9.3 (CVSS 4.0)
CISA	On its exploited list since 15 October 2026. Deadline for US federal agencies: 18 October 2026.
Chance of exploitation (EPSS)	0.99, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Bamboo 10.2.24, 12.1.12; Bitbucket 9.4.26, 10.2.8, 10.5.1; Confluence 10.2.19, 9.2.26; Crowd 7.2.4, 7.1.7, 7.0.3, 6.3.7 (Data Center)
Who looks first	Anyone running Bitbucket, Confluence, Jira Service Management, Jira Software, Bamboo or Crowd Data Center, or Crucible or Fisheye. Internet-facing installations come first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Bitbucket, Confluence, Jira, Bamboo or Crowd Data Center, or Crucible or Fisheye?	Nothing to do for this CVE.	Check the version (next question).
Is your version below the fixed version for your product line?	You are on a fixed release. Ask your provider to confirm it in writing.	Treat it as exposed. Go to the next question.
Can anyone outside your network reach the web address of that product?	Lower urgency, but still patch. Internal users could try the same request.	Restrict external access now, then patch.

Does the product hold sensitive files in its web root, such as configuration or exports?	Risk is lower, but patch anyway.	Move or remove them where you can, and review them as possibly read.

What it is

An attacker with no login can read specific files under the web application's root directory. They must already know the exact file name and path. The flaw does not let them list directories.

Why it matters

The vendor's advisory says sensitive files in some configurations raise the risk, so the impact depends on what sits in the web root. Our reading is that these tools hold source code, documents and credentials, so a readable configuration file could help an attacker go further. The record scores it 9.3 (CVSS 4.0), and the vendor describes it as needing no login.

What the vendor's advisory says

We read three pages on confluence.atlassian.com and jira.atlassian.com. In short:

- The vendor's advisory was released on 5 October 2026 and covers eight Data Center and related products.
- For Bamboo, the vendor says all versions are affected and lists 10.2.24 and 12.1.12 as fixed.
- For Bitbucket Data Center, the vendor lists 9.4.26, 10.2.8 and 10.5.1 as fixed, and says Bitbucket Cloud is not affected.
- The vendor says versions past end of life may also be affected and recommends upgrading to a fixed long-term-support version or later.
- If you cannot patch, the vendor says to take the instance off the internet, or block requests containing '..' next to slashes with a web application firewall rule or proxy rule.

Things people will get wrong

- "They need to know the file path, so it is hard to exploit." The record says only that the exact name and path must be known. It gives no sign that this is hard, and CISA lists the flaw as exploited.
- "We have a login screen, so we are protected." The vendor says instances reachable from the public internet, including those with user authentication, should be restricted. The attacker needs no login.
- "This only affects Bamboo." The record names Bitbucket, Confluence, Jira Service Management, Jira Software, Bamboo, Crowd, Crucible and Fisheye.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find which products and versions you run

- List every Atlassian Data Center product, including old test servers, and note each version.
- Compare each version with the fixed versions in this note.

Step 2: Reduce exposure first

- The vendor says to remove the instance from the internet until you can patch, if possible.
- If you cannot, ask your provider to apply the vendor's firewall or proxy rule, or the product-specific rewrite rule.

```
ss -tlnp
```

Step 3: Patch to a fixed version

- Back up first, then upgrade to a fixed version for your product line.
- Where no source here names a fixed version for your product, ask the vendor. Do not guess one.

Step 4: Check and review

- Get written confirmation of the running version after the upgrade.
- Review web server logs and any sensitive files in the web root, since a read leaves little trace.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to check our exposure to CVE-2026-21589, an unauthenticated file access flaw in Atlassian Data Center products (Bitbucket, Confluence, Jira, Bamboo, Crowd, Crucible, Fisheye). Please tell us which of these we run, where, which version, and whether any can be reached from the internet. If any is below a fixed version, please patch it or restrict access now. CISA's date of 18 October 2026 has passed. Please confirm the version and fix in writing by [date].*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Requests in web server or proxy logs containing '..' next to slashes, including encoded forms.
- Unexpected successful responses for files in the web root from addresses outside your network.
- Sensitive files in the web root that an outsider could have read, such as configuration files.

The weakness behind it

CISA's entry classes this as CWE-552 (Files or Directories Accessible to External Parties).

The sources, in their words

CISA's catalogue entry:

> *Multiple Atlassian products (Bitbucket Data Center ,Confluence Data Center, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center, Crowd Data Center, Crucible and Fisheye) contain a files or directories accessible to external parties vulnerability which could allow an unauthenticated attacker to access specific files within the web application root directory in affected versions.*

The CVE record, published by Atlassian on 5 October 2026:

> *This is a vulnerability in Bitbucket Data Center, Confluence Data Center, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center. Crowd Data Center, Crucible and Fisheye. This Arbitrary File Access vulnerability allows an unauthenticated attacker to access specific files within the web application root directory in affected versions. Exploitation requires prior knowledge of the target file's exact name and path; this vulnerability does not allow attackers to enumerate or list directory contents. In some configurations, there may be some sensitive files that make this highly severe. This vulnerability allows an unauthenticated remote attacker to access specific ...*

Versions of Atlassian Bamboo Data Center the record lists as affected:

- All other versions

It lists these as unaffected:

- Patch version 10.2.24 and later
- Patch version 12.1.12 and later

Versions of Atlassian Bitbucket Data Center the record lists as affected:

- All other versions

It lists these as unaffected:

- Patch version 10.2.8 and later
- Patch version 10.5.1 and later
- Patch version 9.4.26 and later

Versions of Atlassian Confluence Data Center the record lists as affected:

- All other versions

It lists these as unaffected:

- Patch version 10.2.19 and later
- Patch version 9.2.26 and later

Versions of Atlassian Crowd Data Center the record lists as affected:

- All other versions

It lists these as unaffected:

- Patch version 7.2.4 and later
- Patch version 7.1.7 and later
- Patch version 7.0.3 and later
- Patch version 6.3.7 and later

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- The sources do not name fixed versions for Jira Service Management, Jira Software, Crucible or Fisheye.
- They do not say which files attackers have actually read.
- They do not describe how the attacks work or who is behind them.
- They do not say whether the vendor's rewrite rules stop every variant.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-21589: score 9.3, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	None	Nothing can be altered.
Vulnerable system: availability	None	No effect on availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
5 October 2026	CVE record published by Atlassian.
15 October 2026	CISA added it to its list of exploited vulnerabilities.
18 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

An affected version is reachable from the internet, with or without user login	High	Now; CISA's window has passed
An affected version is internal only, reachable by staff and contractors	Medium	This week
The version is end of life and no fixed release exists for it	High	Now; plan an upgrade to a fixed release
You are on a fixed version already	Low	Confirm in writing; no further action
You use only Bitbucket Cloud	None	None for this CVE

Appendix 4. Definition of done

- Every Atlassian Multiple Products you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-21589: https://www.cve.org/CVERecord?id=CVE-2026-21589
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-v: https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html?ref=labs.watchtowr.com
- Advisory or release notes read: jira.atlassian.com/browse/BAM-26567: https://jira.atlassian.com/browse/BAM-26567
- Advisory or release notes read: jira.atlassian.com/browse/BSERV-20604: https://jira.atlassian.com/browse/BSERV-20604
- Reference in the CVE record: jira.atlassian.com: https://jira.atlassian.com/browse/CONFSERVER-104488
- Reference in the CVE record: jira.atlassian.com: https://jira.atlassian.com/browse/CRUC-8741
- Reference in the CVE record: jira.atlassian.com: https://jira.atlassian.com/browse/CWD-6610