



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610060236

NCSC Advisory

Critical Arbitrary File Access Vulnerability
impacting Multiple Atlassian Products

CVE-2026-21589

6th, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>.
Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-21589

Published: 2026-10-05

Vendor: Atlassian

Products: Bamboo Data Center, Bamboo Server, Bitbucket Data Center, Bitbucket Server, Confluence Data Center, Confluence Server, Crowd Data Center, Crowd Server, Crucible Data Center, Crucible Server, Fisheye Data Center, Fisheye Server, Jira Service Management Data Center, Jira Service Management Server, Jira Software Data Center, Jira Software Server

CVSS Score¹: 9.3

Products Affected

Product	Version
Bamboo Data Center	< 10.2.4, < 12.1.12 and all other versions
Bamboo Server	All versions
Bitbucket Data Center	< 9.4.26, < 10.2.8, < 10.5.1 and all other versions
Bitbucket Server	All versions
Confluence Data Center	< 9.2.26, < 10.2.19 and all other versions
Confluence Server	All versions
Crowd Data Center	< 6.3.7, < 7.0.3, < 7.1.1, < 7.2.4 and all other versions
Crowd Server	All versions
Crucible Data Center	< 4.9.15 and all other versions
Crucible Server	< 4.9.15 and all other versions
Fisheye Data Center	< 4.9.15 and all other versions
Fisheye Server	< 4.9.15 and all other versions
Jira Service Management Data Center	< 5.12.40, < 10.3.26, < 11.3.12 and all other versions



Jira Service Management Server	< 5.12.40 and all other versions
Jira Software Data Center	< 9.12.40, < 10.3.26, < 11.3.12 and all other versions
Jira Software Server	< 9.12.40 and all other versions

Impact

This Arbitrary File Access vulnerability allows an unauthenticated remote 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.

Common Weakness Enumeration (CWE)²: N/A

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

¹ <https://www.first.org/cvss/>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Atlassian.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-21589>
- <https://www.cve.org/CVERecord?id=CVE-2026-21589>
- <https://jira.atlassian.com/browse/BAM-26567>
- <https://jira.atlassian.com/browse/BSERV-20604>
- <https://jira.atlassian.com/browse/CONFSERVER-104488>
- <https://jira.atlassian.com/browse/CRUC-8741>
- <https://jira.atlassian.com/browse/CWD-6610>
- <https://jira.atlassian.com/browse/FE-7583>
- <https://jira.atlassian.com/browse/JRASERVER-79546>
- <https://jira.atlassian.com/browse/JSDSERVER-16809>

