



Unauthenticated Remote Arbitrary File Access Vulnerability Found within Atlassian Data Center Products

06 OCT 2026

Unauthorized Access

Crafted HTTP Requests

Mitigation Instructions Available

Fixed Releases Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critically-rated vulnerability found within Atlassian's Data Center Products. The vulnerability, CVE-2026-21589, impacts Bitbucket Data Center, Confluence Data Center, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center, Crowd Data Center, Crucible and Fisheye. CVE-2026-21589 carries a CVSS 4.0 score of 9.3.¹

CVE-2026-21589 stems from the request-handling path of each product's web tier, in that a specially crafted HTTP request causes the application to return the contents of a file residing under the webroot.² The vulnerability enables an unauthenticated remote attacker the ability to read specific files located on that web application root directory of affected Atlassian products. The vulnerability does require prior knowledge of the exact file name and path. Successful exploitation of CVE-2026-21589 leads to disclosure of sensitive information such as configuration files, logs, internal documents – potentially enabling follow-on attacks.³

Atlassian has acknowledged the vulnerability and has issued a security advisory with remediation and temporary mitigation instructions to immediately address it.

The Cal-CSIC recommends following Atlassian's remediation guidance and installing their latest fixed releases as soon as possible.

For additional details regarding CVE-2026-21589, please use this link:

Atlassian Security Advisory:

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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Products and Versions

Product	Affected Version	Fixed Release
Bitbucket Data Center	All Versions Are Affected	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
Fisheye		4.9.15

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Sharing, Reporting, and Support

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:



833-REPORT-1 or 916.636.2997



calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:



Federal Officials at CISA and/or the FBI as applicable



Coordinate with your regional Fusion Center



information, intelligence, and IOCs with ISACs

References

¹ OpenCVE; "CVE-2026-21589"; <https://app.opencve.io/cve/CVE-2026-21589>; accessed 06 October 6, 2026

¹ Security Arsenal; "CVE-2026-21589: Atlassian Data Center Arbitrary File Read Across 8 Products — Detection and Remediation Guide"; <https://securityarsenal.com/blog/cve-2026-21589-atlassian-data-center-arbitrary-file-read-across-8-products-detection-and-remediation-guide>; accessed 06 October 6, 2026

¹ Atlassian Support; "CVE-2026-21589 – Arbitrary File Access Vulnerability impacts Multiple Products"; CVE-2026-21589 - Arbitrary File Access Vulnerability impacts Multiple Products | Atlassian Support | Atlassian Documentation; accessed 06 October 2026

¹ OpenCVE; "CVE-2026-21589"; <https://app.opencve.io/cve/CVE-2026-21589>; accessed 06 October 6, 2026

² Security Arsenal; "CVE-2026-21589: Atlassian Data Center Arbitrary File Read Across 8 Products — Detection and Remediation Guide"; <https://securityarsenal.com/blog/cve-2026-21589-atlassian-data-center-arbitrary-file-read-across-8-products-detection-and-remediation-guide>; accessed 06 October 6, 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

³ Atlassian Support; “CVE-2026-21589 – Arbitrary File Access Vulnerability impacts Multiple Products”; CVE-2026-21589 - Arbitrary File Access Vulnerability impacts Multiple Products | Atlassian Support | Atlassian Documentation; accessed 06 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.