



CVE-2020-29445

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-29445
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-07 06:15:00 UTC
Updated	2022-05-13 20:53:00 UTC
Description	Affected versions of Confluence Server before 7.4.8, and versions from 7.5.0 before 7.11.0 allow attackers to identify intern

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Confluence	All	All	All	All
Application	Atlassian	Confluence Server	All	All	All	All

References

Reference

[CONFSERVER-61453] Blind SSRF in Team Calendars REST API using location parameter - CVE-2020-29445 - Create and track feature rec

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730471](#) Atlassian Confluence Blind Server Side Request Forgery (SSRF) Vulnerability (CONFSERVER-61453)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)