



CVE-2020-36290

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

Summary

CVE	CVE-2020-36290
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-26 04:15:00 UTC
Updated	2022-08-01 16:21:00 UTC
Description	The Livesearch macro in Confluence Server and Data Center before version 7.4.5, from version 7.5.0 before 7.6.3, and from

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

[CONFSERVER-60118] Stored XSS in the Livesearch macro - CVE-2020-36290 - Create and track feature requests for Atlassian products.

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)