



CVE-2020-24897

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

Summary

CVE	CVE-2020-24897
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-29 20:15:00 UTC
Updated	2020-09-04 16:53:00 UTC
Description	The Table Filter and Charts for Confluence Server app before 5.3.25 (for Atlassian Confluence) allow remote attackers to ir

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Stiltsoft	Table Filter And Charts For Confluence Server	All	All	All	All
Application	Stiltsoft	Table Filter And Charts For Confluence Server	All	All	All	All

References

Reference	Source
[VD-2] Cross-site scripting (XSS) in Table from CSV macro (Table Filter and Charts for Confluence Server) - CVE-2020-24897 - JIRA	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report