



# CVE-2021-43956

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

## Summary

<b>CVE</b>	CVE-2021-43956
<b>State</b>	PUBLIC
<b>Assigner</b>	security@atlassian.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-16 01:15:00 UTC
<b>Updated</b>	2022-03-22 16:01:00 UTC
<b>Description</b>	The jQuery deserialize library in Fisheye and Crucible before version 4.8.9 allowed remote attackers to to inject arbitrary HT

## Risk And Classification

**Problem Types:** CWE-1321

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All

## References

### Reference

[FE-7395] CVE-2021-43956: Javascript Prototype Pollution in the jQuery deserialize library - Create and track feature requests for Atlassian p

[CRUC-8531] CVE-2021-43956: Javascript Prototype Pollution in the jQuery deserialize library - Create and track feature requests for Atlassia

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.

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](#)**