



CVE-2021-26723

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

Summary

CVE	CVE-2021-26723
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-06 06:15:00 UTC
Updated	2021-03-04 21:45:00 UTC
Description	Jenzabar 9.2.x through 9.2.2 allows /ics?tool=search&query= XSS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenzabar	Jenzabar	All	All	All	All

References

Reference	Score
Higher Education Blog Management Software & ERP Solutions Jenzabar - The latest news and trends in higher education technology	MI
XSS in Jenzabar(CVE-2021-26723). # Exploit Title: Jenzabar 9.2.x through... by y0ung_dst Feb, 2021 Medium	MI
Jenzabar 9.2.2 Cross Site Scripting ≈ Packet Storm	MI
CVE-2021-26723 · GitHub	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

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