



CVE-2021-3224

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

Summary

CVE	CVE-2021-3224
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-10 14:15:00 UTC
Updated	2021-03-12 00:58:00 UTC
Description	A stored cross-site scripting (XSS) vulnerability in cszcms 1.2.9 exists in /admin/pages/new via the content parameter.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cszcms	Csz Cms	1.2.9	All	All	All
Application	Cszcms	Csz Cms	1.2.9	All	All	All

References

Reference	Source	Link	Tags
Stored XSS Vulnerability In /admin/pages/new (release/1.2.9) · Issue #28 · cskaza/cszcms · GitHub	MISC	github.com	Exploi
Open Source CMS Codeigniter Bootstrap CSZ CMS Official Website	MISC	www.cszcms.com	Produ
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

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