



CVE-2021-41747

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

Summary

CVE	CVE-2021-41747
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-22 12:15:00 UTC
Updated	2021-10-25 18:24:00 UTC
Description	Cross-Site Scripting (XSS) vulnerability exists in Csdn APP 4.10.0, which can be exploited by attackers to obtain sensitive i

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Csdn	Csdn App	4.10.0	All	All	All

References

Reference	Source	Link	Tags
Security-vulnerability/Csdn APP 4.10.0 XSS at main · purple-WL/Security-vulnerability · GitHub	MISC	github.com	
www.cnvd.org.cn/flaw/show/CNVD-2021-52394	MISC	www.cnvd.org.cn	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

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