



CVE-2022-48013

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

Summary

CVE	CVE-2022-48013
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-27 18:15:00 UTC
Updated	2023-02-04 01:53:00 UTC
Description	Opencats v0.9.7 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /opencats/index

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencats	Opencats	0.9.7	All	All	All

References

Reference

- [Opencats-0.9.7-Vulnerabilities/Opencats-0.9.7-Stored XSS in Calendar-Add-Event.md at main · Sakura-501/Opencats-0.9.7-Vulnerabilities · C](#)
- [GitHub - Sakura-501/Opencats-0.9.7-Vulnerabilities: Opencats-0.9.7-Vulnerabilities](#)
- [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.

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