



CVE-2023-4829

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

Summary

CVE	CVE-2023-4829
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-13 13:15:00 UTC
Updated	2023-10-17 16:10:00 UTC
Description	Cross-site Scripting (XSS) - Stored in GitHub repository froxlor/froxlor prior to 2.0.22.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
correct validation of hostingplan name and description · Froxlor/Froxlor@4711a41 · GitHub	MISC	github.com	
Stored HTML injection vulnerability found in froxlor	MISC	huntr.dev	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995569 PHP (Composer) Security Update for froxlor/froxlor (GHSA-cvww-h85m-w37h)

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