



CVE-2022-23872

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

Summary

CVE	CVE-2022-23872
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-31 22:15:00 UTC
Updated	2022-09-30 14:49:00 UTC
Description	Emlog pro v1.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /admin/config

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emlog	Emlog	1.1.1	All	All	All
Application	Emlog	Emlog Pro	1.1.1	All	All	All

References

Reference	Source	Link
GitHub - truonghuuphuc/CVE: All of my found cves	MISC	github.com
Emlog pro-1.1.1 has xss stored in /admin/configure.php via footer_info param. · Issue #147 · emlog/emlog · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)