CVE-2026-2728

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-2728
State	PUBLISHED
Assigner	PRJBLK
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 11:16:05 UTC
Updated	2026-04-22 19:46:01 UTC
Description	LibreNMS versions before 26.3.0 are affected by an authenticated Cross-site Scripting vulnerability on the showconfig page

Risk And Classification

Primary CVSS: v4.0 4.6 MEDIUM from ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000020000 probability, percentile 0.000520000 (date 2026-04-22)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
4.0	ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a	Secondary	4.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N
4.0	CNA	CVSS	4.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Active

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Librenms	Librenms	affected 26.3.0 custom	Not specified

References

Reference	Source	Link	Tags
projectblack.io/blog/librenms-authenticated-rce-and-xss	ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a	projectblack.io	Exploit, Third Party Ad
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.

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