CVE-2026-6204

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

Summary

CVE	CVE-2026-6204
State	PUBLISHED
Assigner	PRJBLK
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 11:16:06 UTC
Updated	2026-04-22 19:47:46 UTC
Description	LibreNMS versions before 26.3.0 are affected by an authenticated remote code execution vulnerability by abusing the Binar

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/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: 0.000060000 probability, percentile 0.004070000 (date 2026-04-22)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper neutralization of special elements used in an OS command ('OS command injection')

Version	Source	Type	Score	Severity	Vector
4.0	ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a	Secondary	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/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

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

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
github.com/librenms/librenms/security/advisories/GHSA-pr3g-phhr-h8fh	ab69c47f-b95e-4bf2-b2d9-4b1fd1b24b4a	github.com	Third F
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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