



CVE-2026-41254

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-41254
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-18 07:16:10 UTC
Updated	2026-04-22 18:34:23 UTC
Description	Little CMS (lcms2) through 2.18 has an integer overflow in CubeSize in cmslut.c because the overflow check is performed a

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.000170000 probability, percentile 0.044340000 (date 2026-04-22)

Problem Types: CWE-696 | CWE-190 | CWE-696 CWE-696 Incorrect Behavior Order

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	cve@mitre.org	Secondary	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L
3.1	CNA	CVSS	4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Littlecms	Little Cms	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Littlecms	Little Cms Color Engine	affected 2.18 custom	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/17/16	cve@mitre.org	www.openwall.com	Mailin
github.com/mm2/Little-CMS/commit/da6110b1d14abc394633a388209abd5ebdd7ab0	cve@mitre.org	github.com	Patch
github.com/mm2/Little-CMS/security/advisories/GHSA-4xp6-rcgg-m9qq	cve@mitre.org	github.com	Brok
abhinavagarwal07.github.io/posts/lcms2-cubeseize-overflow	cve@mitre.org	abhinavagarwal07.github.io	Explo
github.com/mm2/Little-CMS/commit/e0641b1828d0a1af5ecb1b11fe22f24fceedf4bc	cve@mitre.org	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report