



mackron / dr_libs dr_flac.h Excessive Memory Allocation in PICTURE Metadata Parsing

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

Summary

CVE	CVE-2026-32836
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-17 20:16:14 UTC
Updated	2026-04-27 16:16:43 UTC
Description	dr_libs dr_flac.h version 0.13.3 and earlier (fixed in commits fefced4, 4f5a4cd, and 663239a) contain an uncontrolled memo

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000150000 probability, percentile 0.033370000 (date 2026-04-27)

Problem Types: CWE-789 | CWE-789 CWE-789 Memory allocation with excessive size value

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	disclosure@vulncheck.com	Primary	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.2	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/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	Mackron	Dr Libs	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mackron	Dr Libs Dr Flac.h	affected 0.13.3 semver	Not specified
CNA	Mackron	Dr Libs Dr Flac.h	affected fefced4a64adfb1a68a2d31d882366e56096dee8 git	Not specified
CNA	Mackron	Dr Libs Dr Flac.h	affected 4f5a4cd3b57564d969443c580c75857e039f100a git	Not specified
CNA	Mackron	Dr Libs Dr Flac.h	affected 663239a3d0460c33bd5b6e5166edcb404e3df676 git	Not specified

References

Reference	Source	Link
github.com/mackron/dr_libs/commit/4f5a4cd3b57564d969443c580c75857e039f100a	disclosure@vulncheck.com	github.com
github.com/mackron/dr_libs/commit/663239a3d0460c33bd5b6e5166edcb404e3df676	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/mackron-dr-libs-excessive-memory-allocation-in-pic...	disclosure@vulncheck.com	www.vulncheck.com
github.com/mackron/dr_libs/commit/fefced4a64adfb1a68a2d31d882366e56096dee8	disclosure@vulncheck.com	github.com
github.com/mackron/dr_libs/issues/298	disclosure@vulncheck.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Ana Kapulica (en)

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](#)