



libvips source.c vips_source_read_to_memory heap-based overflow

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

Summary

CVE	CVE-2026-2913
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-22 04:15:59 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was determined in libvips up to 8.19.0. The affected element is the function vips_source_read_to_memory of

Risk And Classification

Primary CVSS: v4.0 1.1 LOW from cna@vulldb.com

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

Problem Types: CWE-119 | CWE-122 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	1.1	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	2	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	2.5	LOW	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
2.0	cna@vulldb.com	Secondary	1		AV:L/AC:H/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	1		AV:L/AC:H/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/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

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C



NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Libvips	affected 8.0	Not specified
CNA	Na	Libvips	affected 8.1	Not specified
CNA	Na	Libvips	affected 8.2	Not specified
CNA	Na	Libvips	affected 8.3	Not specified
CNA	Na	Libvips	affected 8.4	Not specified
CNA	Na	Libvips	affected 8.5	Not specified
CNA	Na	Libvips	affected 8.6	Not specified
CNA	Na	Libvips	affected 8.7	Not specified
CNA	Na	Libvips	affected 8.8	Not specified
CNA	Na	Libvips	affected 8.9	Not specified
CNA	Na	Libvips	affected 8.10	Not specified
CNA	Na	Libvips	affected 8.11	Not specified
CNA	Na	Libvips	affected 8.12	Not specified
CNA	Na	Libvips	affected 8.13	Not specified
CNA	Na	Libvips	affected 8.14	Not specified

CNA	Na	Libvips	affected 8.15	Not specified
CNA	Na	Libvips	affected 8.16	Not specified
CNA	Na	Libvips	affected 8.17	Not specified
CNA	Na	Libvips	affected 8.18	Not specified
CNA	Na	Libvips	affected 8.19.0	Not specified

References			
Reference	Source	Link	Tags
github.com/libvips/libvips/issues/4857	cna@vuldb.com	github.com	Exploit, Issue Tracking
github.com/libvips/libvips/commit/a56feecbe9ed66521d9647ec9fbcd2546eccd7ee	cna@vuldb.com	github.com	Patch
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, V
github.com/libvips/libvips/issues/4857	cna@vuldb.com	github.com	Issue Tracking
github.com/libvips/libvips/issues/4857	cna@vuldb.com	github.com	Exploit, Issue Tracking
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Required,
github.com/libvips/libvips	cna@vuldb.com	github.com	Product
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory, V
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit
Discovery Credit
CNA: Niebelungen (VulDB User) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2026-02-20T00:00:00.000Z	Advisory disclosed
CNA	2026-02-20T01:00:00.000Z	VulDB entry created
CNA	2026-02-20T21:26:01.000Z	VulDB entry last update

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

[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