SDL_image has a heap buffer overflow READ via unchecked colormap index in XCF loader

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

Summary

CVE	CVE-2026-35444
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 22:16:23 UTC
Updated	2026-04-16 04:41:25 UTC
Description	SDL_image is a library to load images of various formats as SDL surfaces. In do_layer_surface() in src/IMG_xcf.c, pixel ind

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

EPSS: 0.000110000 probability, percentile 0.014290000 (date 2026-04-20)

Problem Types: CWE-125 | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L
3.1	security-advisories@github.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

None

vailability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libsdl	Sdl Image	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Libsdl-org	SDL Image	affected < 996bf12888925932daace576e09c30534108 96f8	Not specified

References

Reference	Source	Link	Tags
github.com/libsdl-org/SDL_image/security/advisories/GHSA-gq8w-x74c-h6p7	security-advisories@github.com	github.com	Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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