Heap buffer overflow READ via unchecked colormap index in XCF loader

High **slouken** published **GHSA-gq8w-x74c-h6p7** 4 days ago

Package

SDL_image

Affected versions

all versions prior to commit 996bf12

Patched versions

Patched in: 996bf12888925932daace576e09c3053410896f8

Description

In do_layer_surface() in src/IMG_xcf.c, pixel index values from decoded XCF tile data are used directly as colormap indices without validating them against the colormap size (cm_num). A crafted .xcf file with a small colormap and out-of-range pixel indices causes heap out-of-bounds reads of up to 762 bytes past the colormap allocation.

Both IMAGE_INDEXED code paths are affected (bpp=1 and bpp=2). The leaked heap bytes are written into the output surface pixel data, making them potentially observable in the rendered image.

ASAN-confirmed on x86_64 and aarch64.

Patched in: `996bf12`

Credit: Sebastián Alba Vives (@**Sebasteuo**)

Severity

High 7.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	Low

Learn more about base metrics

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

CVE ID

CVE-2026-35444

Weaknesses

▶ CWE-125

Credits

Sebasteuo Reporter