heap-buffer-overflow in function ttULONG() at stb_truetype.h:1288 #1288

Closed **Vincebye** opened this issue on Feb 16 · 1 comment

Vincebye commented on Feb 16

Describe
A heap-buffer-overflow was discovered in stb_truetype. The issue is being triggered in function ttLONG() at stb_truetype.h:1288
To Reproduce
test program

```
#include <stdio.h>
#include <stdlib.h>
#define STB_IMAGE_WRITE_IMPLEMENTATION
#include "stb_image_write.h"
#define STB_TRUETYPE_IMPLEMENTATION
#include "stb_truetype.h"
int main(int argc, const char *argv[])
{
    long int size = 0;
    unsigned char *fontBuffer = NULL;
    FILE *fontFile = fopen(argv[1], "rb");
    if (fontFile == NULL)
    {
        printf("Can not open font file!\n");
        return 0;
    }
    fseek(fontFile, 0, SEEK_END);
    size = ftell(fontFile);
    fseek(fontFile, 0, SEEK_SET);
    fontBuffer = calloc(size, sizeof(unsigned char));
    fread(fontBuffer, size, 1, fontFile);
    fclose(fontFile);
    stbtt_fontinfo info;
    if (!stbtt_InitFont(&info, fontBuffer, 0))
    {
        printf("stb init font failed\n");
    }
    int bitmap_w = 512;
```

```
    int bitmap_h = 128;
    free(fontBuffer);
    return 0;
}
```

Compile test program with address sanitizer with this command:

```
AFL_HARDEN=1 afl-gcc -I /src/stb/include ttf.c -o ttf -lm
```

You can get program here

Asan Reports

```
./Asanttf crash/45
```

Get ASan reports

```
==3168==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x610000000104 at pc
0x55700d9d677b bp 0x7ffd59f491f0 sp 0x7ffd59f491e0
READ of size 1 at 0x610000000104 thread T0
    #0 0x55700d9d677a in ttULONG /src/stb/include/stb_truetype.h:1288
    #1 0x55700d9d6d05 in stbtt__find_table /src/stb/include/stb_truetype.h:1314
    #2 0x55700d9f6e49 in stbtt_InitFont_internal /src/stb/include/stb_truetype.h:1393
    #3 0x55700d9f6e49 in stbtt_InitFont /src/stb/include/stb_truetype.h:4954
    #4 0x55700d9f91fc in main /src/stb/ttf.c:32
    #5 0x7fd105b7e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #6 0x55700d9d270d in _start (/src/stb/Asanttf+0x470d)

0x610000000104 is located 4 bytes to the right of 192-byte region [0x610000000040,0x610000000100)
allocated by thread T0 here:
    #0 0x7fd105f4ce17 in __interceptor_calloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
    #1 0x55700d9f91c6 in main /src/stb/ttf.c:26
    #2 0x7fd105b7e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/stb/include/stb_truetype.h:1288 in ttULONG
Shadow bytes around the buggy address:
  0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c207fff8020:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
```

```
    Stack after return:      f5
    Stack use after scope:   f8
    Global redzone:          f9
    Global init order:       f6
    Poisoned by user:        f7
    Container overflow:      fc
    Array cookie:            ac
    Intra object redzone:    bb
    ASan internal:           fe
    Left alloca redzone:     ca
    Right alloca redzone:    cb
    Shadow gap:              cc
  ==3168==ABORTING
```

Poc

Poc file is here

nothings commented on Feb 17 — Owner

see #1286

nothings closed this as completed on Feb 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants