New issue

Jump to bottom

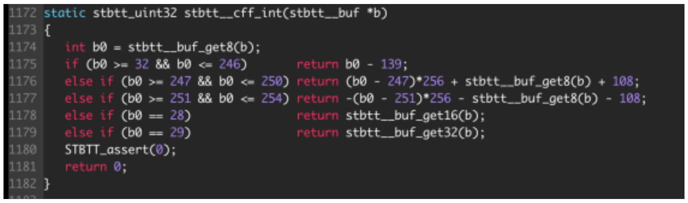
assertion failure in stbtt__cff_int in stb_truetype.h #864

Closed **sleicasper** opened this issue on Jan 6, 2020 · 2 comments

Labels 1 stb_truetype

sleicasper commented on Jan 6, 2020

assertion failure in `stbtt__cff_int` can be triggered by user supplied font file.



```
1172 static stbtt_uint32 stbtt__cff_int(stbtt__buf *b)
1173 {
1174    int b0 = stbtt__buf_get8(b);
1175    if (b0 >= 32 && b0 <= 246)       return b0 - 139;
1176    else if (b0 >= 247 && b0 <= 250) return (b0 - 247)*256 + stbtt__buf_get8(b) + 108;
1177    else if (b0 >= 251 && b0 <= 254) return -(b0 - 251)*256 - stbtt__buf_get8(b) - 108;
1178    else if (b0 == 28)               return stbtt__buf_get16(b);
1179    else if (b0 == 29)               return stbtt__buf_get32(b);
1180    STBTT_assert(0);
1181    return 0;
1182 }
```

poc:
poc.zip

result:

```
#0  __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff6e43801 in __GI_abort () at abort.c:79
#2  0x00007ffff6e3339a in __assert_fail_base (fmt=0x7ffff6fba7d8 "%s%s%s:%u: %s%sAssertion `%s' failed.\n%n",
    assertion=assertion@entry=0x505b00 <.str> "0", file=file@entry=0x505b40 <.str> "./SRC/stb_truetype.h",
    line=line@entry=0x49c,
    function=function@entry=0x5063c0 <__PRETTY_FUNCTION__.stbtt__cff_int> "stbtt_uint32 stbtt__cff_int(stbtt__buf *)")
    at assert.c:92
#3  0x00007ffff6e33412 in __GI___assert_fail (assertion=0x505b00 <.str> "0",
    file=0x505b40 <.str> "./SRC/stb_truetype.h", line=0x49c,
    function=0x5063c0 <__PRETTY_FUNCTION__.stbtt__cff_int> "stbtt_uint32 stbtt__cff_int(stbtt__buf *)")
    at assert.c:101
#4  0x00000000004e7c73 in stbtt__cff_int (b=0x7fffffffd980) at ./SRC/stb_truetype.h:1180
#5  0x00000000004ea9e6 in stbtt__cff_skip_operand (b=0x7fffffffd980) at ./SRC/stb_truetype.h:1195
#6  0x00000000004ea430 in stbtt__dict_get (b=0x7fffffffd980, key=0x11) at ./SRC/stb_truetype.h:1205
#7  0x00000000004e9bc3 in stbtt__dict_get_ints (b=0x7fffffffd980, key=0x11, outcount=0x1, out=0x7fffffffd9d0)
    at ./SRC/stb_truetype.h:1217
#8  0x00000000004e0924 in stbtt_InitFont_internal (info=0x7fffffffe1c0, data=0x629000000200 "OTTO", fontstart=0x0)
    at ./SRC/stb_truetype.h:1386
#9  0x00000000004d71a3 in stbtt_InitFont (info=0x7fffffffe1c0, data=0x629000000200 "OTTO", offset=0x0)
    at ./SRC/stb_truetype.h:4771
#10 0x00000000004e1b29 in main (argc=0x2, argv=0x7fffffffe458) at ../fuzzsrc/ttfuzz.c:29
#11 0x00007ffff6e24b97 in __libc_start_main (main=0x4e18f0 <main>, argc=0x2, argv=0x7fffffffe458,
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe448)
    at ../csu/libc-start.c:310
#12 0x000000000041ad4a in _start ()
```

carnil commented on Jan 10, 2020

CVE-2020-6617 was assigned for this issue.

nothings added the 1 stb_truetype label on Feb 1, 2020

nothings commented on Jul 4, 2021 Owner

The documentation for the library was modified in 2020 to make clear it is intentionally insecure, and fixing issues like this is out of scope.

nothings closed this as completed on Jul 4, 2021

Assignees

No one assigned

Labels

1 stb_truetype

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants