New issue

Jump to bottom

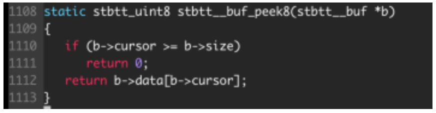
heap overflow in stbtt__buf_peek8 in stb_truetype.h #869

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

Labels 1 stb_truetype

sleicasper commented on Jan 6, 2020

heap overflow in `stbtt__buf_peek8` .



```
static stbtt_uint8 stbtt__buf_peek8(stbtt__buf *b)
{
   if (b->cursor >= b->size)
      return 0;
   return b->data[b->cursor];
}
```

poc:
poc.zip

result:

```
=================================================================
==26964==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62900000c545 at pc 0x0000004ea862 bp 0x7fffffffd2a0 sp 0x7fffffffd298
READ of size 1 at 0x62900000c545 thread T0
    #0 0x4ea861  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4ea861)
    #1 0x4ea417  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4ea417)
    #2 0x4e9bc2  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e9bc2)
    #3 0x4e9768  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e9768)
    #4 0x4e0aa9  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e0aa9)
    #5 0x4d71a2  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4d71a2)
    #6 0x4e1b28  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e1b28)
    #7 0x7ffff6e24b96  (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x41ad49  (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x41ad49)

Address 0x62900000c545 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4ea861)
Shadow bytes around the buggy address:
  0x0c527fff9850: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9860: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9870: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9880: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9890: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c527fff98a0: fa fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa
  0x0c527fff98b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff98c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff98d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff98e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff98f0: 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
==26964==ABORTING

Program received signal SIGABRT, Aborted.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x73be28 --> 0x0
RCX: 0x7ffff6e41e97 (<__GI_raise+199>:  mov    rcx,QWORD PTR [rsp+0x108])
RDX: 0x0
RSI: 0x7fffffffc2e0 --> 0x0
RDI: 0x2
RBP: 0x7fffffffd270 --> 0x7fffffffd2a0 --> 0x7fffffffd310 --> 0x7fffffffd490 --> 0x7fffffffd5d0 --> 0x7fffffffd8d0 (--> ...)
RSP: 0x7fffffffc2e0 --> 0x0
RIP: 0x7ffff6e41e97 (<__GI_raise+199>:  mov    rcx,QWORD PTR [rsp+0x108])
R8 : 0x0
R9 : 0x7fffffffc2e0 --> 0x0
R10: 0x8
R11: 0x246
R12: 0x7fffffffd2a0 --> 0x7fffffffd310 --> 0x7fffffffd490 --> 0x7fffffffd5d0 --> 0x7fffffffd8d0 --> 0x7fffffffe120 (--> ...)
R13: 0x7fffffffd298 --> 0x7fffffffd1a0 --> 0x45e0360e
R14: 0x7fffffffd240 --> 0x7ffffffff014c --> 0x0
R15: 0x7ce288 --> 0x1
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff6e41e8b <__GI_raise+187>:     mov    edi,0x2
   0x7ffff6e41e90 <__GI_raise+192>:     mov    eax,0xe
   0x7ffff6e41e95 <__GI_raise+197>:     syscall
=> 0x7ffff6e41e97 <__GI_raise+199>:     mov    rcx,QWORD PTR [rsp+0x108]
   0x7ffff6e41e9f <__GI_raise+207>:     xor    rcx,QWORD PTR fs:0x28
   0x7ffff6e41ea8 <__GI_raise+216>:     mov    eax,r8d
   0x7ffff6e41eab <__GI_raise+219>:     jne    0x7ffff6e41ecc <__GI_raise+252>
   0x7ffff6e41ead <__GI_raise+221>:     add    rsp,0x118
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffc2e0 --> 0x0
0008| 0x7fffffffc2e8 --> 0x7496836615c70b4b
0016| 0x7fffffffc2f0 --> 0x0
0024| 0x7fffffffc2f8 --> 0x0
0032| 0x7fffffffc300 --> 0x0
0040| 0x7fffffffc308 --> 0x0
0048| 0x7fffffffc310 --> 0x0
0056| 0x7fffffffc318 --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGABRT
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
51      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
gdb-peda$ bt
#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  0x00000000004b0707 in __sanitizer::Abort() ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/sanitizer_common/sanitizer_posix_libcdep.cc:154
#3  0x00000000004af0e1 in __sanitizer::Die() ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/sanitizer_common/sanitizer_termination.cc:58
#4  0x0000000000496c69 in ~ScopedInErrorReport ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_report.cc:186
#5  0x00000000004983df in ReportGenericError ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_report.cc:470
#6  0x0000000000498ab8 in __asan_report_load1 () at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_rtl.cc:117
#7  0x00000000004ea862 in stbtt__buf_peek8 (b=0x7fffffffd690) at ./SRC/stb_truetype.h:1112
#8  0x00000000004ea418 in stbtt__dict_get (b=0x7fffffffd690, key=0x13) at ./SRC/stb_truetype.h:1204
#9  0x00000000004e9bc3 in stbtt__dict_get_ints (b=0x7fffffffd690, key=0x13, outcount=0x1, out=0x7fffffffd660)
    at ./SRC/stb_truetype.h:1217
#10 0x00000000004e9769 in stbtt__get_subrs (cff=..., fontdict=...) at ./SRC/stb_truetype.h:1329
#11 0x00000000004e0aaa in stbtt_InitFont_internal (info=0x7fffffffe180, data=0x629000000200 "OTTO", fontstart=0x0)
    at ./SRC/stb_truetype.h:1390
#12 0x00000000004d71a3 in stbtt_InitFont (info=0x7fffffffe180, data=0x629000000200 "OTTO", offset=0x0)
    at ./SRC/stb_truetype.h:4771
#13 0x00000000004e1b29 in main (argc=0x2, argv=0x7fffffffe428) at ../fuzzsrc/ttfuzz.c:29
#14 0x00007ffff6e24b97 in __libc_start_main (main=0x4e18f0 <main>, argc=0x2, argv=0x7fffffffe428,
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe418)
    at ../csu/libc-start.c:310
#15 0x000000000041ad4a in _start ()
```

carnil commented on Jan 10, 2020

CVE-2020-6622 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