

[Jump to bottom](#)

✔ Closed

sleicasper opened this issue on Jan 6, 2020 · 4 comments

1 stb_truetype

heap overflow in line 1281. stbtt_find_table doesn't check any out of bound access, so heap overflow can be triggered here.

рост:

poc.zip

result:

0x6020000002c is located 12 bytes to the right of 16-byte region [0x60200000010,0x60200000020) allocated by thread T0 here:

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4c96c9)

Shadow bytes around the buggy address:

```
0x0c047ffff7f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047ffff7fc: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047ffff7fd: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047ffff7fe: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047ffff7ff: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047ffff800: fa fa 00 00 fa[fa]fa fa fa fa fa fa fa fa fa
0x0c047ffff810: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047ffff820: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047ffff830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047ffff840: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047ffff850: 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

```

Program received signal SIGABRT, Aborted.

b

```
[-----registers-----]
```

RAX: 0x0

RBX: 0x73be28 --> 0x0

RCX: 0x74

RDX: 0x0

RSI: 0x7f

RDI: 0x2

RBP: 0x7f

RSP: 0x7f

RIP: 0x7f

R8 : 0x0

R9 : 0x74

R10: 0x8

R11: 0x24

R13: 0x74

R13: 0x74

R13. 0x7f

```

R14: 0x7fffffff7a0 --> 0x45e0010e
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| 0x7ffff6c840 --> 0x0
0008| 0x7ffff6c848 --> 0x0
0016| 0x7ffff6c850 --> 0x0
0024| 0x7ffff6c858 --> 0x0
0032| 0x7ffff6c860 --> 0x0
0040| 0x7ffff6c868 --> 0x0
0048| 0x7ffff6c870 --> 0x0
0056| 0x7ffff6c878 --> 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  0x0000ffff6e43801 in __GI_abort () at abort.c:79
#2  0x0000000004b0707 in __sanitizer::Abort() ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/sanitizer_common/sanitizer_posix_libcdep.cc:154
#3  0x0000000004af0e1 in __sanitizer::Die() ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/sanitizer_common/sanitizer_termination.cc:58
#4  0x000000000496c69 in ~ScopedInErrorReport ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_report.cc:186
#5  0x0000000004983df in ReportGenericError ()
    at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_report.cc:470
#6  0x000000000498ab8 in __asan_report_load1 () at /tmp/final/llvm.src/projects/compiler-rt/lib/asan/asan_rtl.cc:117
#7  0x0000000004c96ca in stbtt__find_table (data=0x602000000010 "wOF2\200\001", fontstart=0x0,
    tag=0x5071a0 <.str> "cmap") at ./SRC/stb_truetype.h:1281
#8  0x0000000004df962 in stbtt_InitFont_internal (info=0x7ffff6ffe180, data=0x602000000010 "wOF2\200\001",
    fontstart=0x0) at ./SRC/stb_truetype.h:1344
#9  0x0000000004d71a3 in stbtt_InitFont (info=0x7ffff6ffe180, data=0x602000000010 "wOF2\200\001", offset=0x0)
    at ./SRC/stb_truetype.h:4771
#10 0x0000000004e1b29 in main (argc=0x2, argv=0x7ffff6ffe428) at ../fuzzsrc/ttfuzz.c:29
#11 0x00007ffff6e24b97 in __libc_start_main (main=0x4e18f0 <main>, argc=0x2, argv=0x7ffff6ffe428,
    init=<optimized out>, fini=<optimized out>, rtdl_fini=<optimized out>, stack_end=0x7ffff6ffe418)
    at ../csu/libc-start.c:310
#12 0x00000000041ad4a in _start ()

```

carnil commented on Jan 10, 2020

[CVE-2020-6618](#) was assigned for this issue.

NicoleG25 commented on Jan 12, 2020

@nothings is there any plans to address this vulnerability ? :)
Cheers !


nothings commented on Jan 12, 2020

Owner

@NicoleG25 It will be addressed eventually but it's not a priority.

The stb libraries were originally written for game developers who had control over their input files and therefore vulnerabilities like this weren't really important.


While stb_image has been improving, stb_truetype probably just needs a thorough going over since there are probably dozens or hundreds of places in the code where offsets are loaded from the file but aren't validated. So, that will happen someday. But a denial-of-service attack if you have control over the fonts being loaded by a program just isn't very high priority to me, considering the dozens of other bugs currently outstanding.

 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

4 participants

