

[New issue](#)[Jump to bottom](#)

heap overflow in ttUSHORT in stb_truetype.h #867

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

Labels

1 stb_truetype

sleicasper commented on Jan 6, 2020

ttUSHORT don't have any bound check, so heap overflow can be triggered.

```
1254 static stbtt_uint16 ttUSHORT(stbtt_uint8 *p) { return p[0]*256 + p[1]; }
1255 static stbtt_int16 ttSHORT(stbtt_uint8 *p) { return p[0]*256 + p[1]; }
1256 static stbtt_uint32 ttULONG(stbtt_uint8 *p) { return (p[0]<<24) + (p[1]<<16) + (p[2]<<8) + p[3]; }
1257 static stbtt_int32 ttLONG(stbtt_uint8 *p) { return (p[0]<<24) + (p[1]<<16) + (p[2]<<8) + p[3]; }
1258
```

```
1417 numTables = ttUSHORT(data + cmap + 2);
1418 info->index_map = 0;
1419 for (i=0; i < numTables; ++i) {
1420     stbtt_uint32 encoding_record = cmap + 4 + 8 * i;
1421     // find an encoding we understand:
1422     switch(ttUSHORT(data+encoding_record)) {
1423         case STBTT_PLATFORM_ID_MICROSOFT:
1424             switch (ttUSHORT(data+encoding_record+2)) {
1425                 case STBTT_MS_EID_UNICODE_BMP:
1426                 case STBTT_MS_EID_UNICODE_FULL:
1427                     // MS/Unicode
1428                     info->index_map = cmap + ttULONG(data+encoding_record+4);
1429                     break;
1430             }
1431             break;
1432         case STBTT_PLATFORM_ID_UNICODE:
1433             // Mac/iOS has these
1434             // all the encodingIDs are unicode, so we don't bother to check it
1435             info->index_map = cmap + ttULONG(data+encoding_record+4);
1436             break;
1437     }
1438 }
```

poc:

[poc.zip](#)

result:

```
=====
==59598==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6190000004dc at pc 0x0000004c2b5b bp 0x7fffffffdb90 sp 0x7fffffffdb88
READ of size 1 at 0x6190000004dc thread T0
#0 0x4c2b5a (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4c2b5a)
#1 0x4e13c0 (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e13c0)
#2 0x4d71a2 (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4d71a2)
#3 0x4e1b28 (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e1b28)
#4 0x7ffff6e24b96 (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#5 0x41ad49 (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x41ad49)

0x6190000004dc is located 4 bytes to the right of 1112-byte region [0x619000000080,0x6190000004d8)
allocated by thread T0 here:
#0 0x492c4d (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x492c4d)
#1 0x4e1ac8 (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4e1ac8)
#2 0x7ffff6e24b96 (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/casper/targets/struct/stb/dbg/fuzzrun/ttfuzz+0x4c2b5a)
Shadow bytes around the buggy address:
 0x0c327fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
->0x0c327fff8090: 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
 0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fff80e0: 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
==59598==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: 0x7fffffc8d0 --> 0x0
RDI: 0x2
RBP: 0x7fffffd860 --> 0x7fffffd890 --> 0x7fffffd8d0 --> 0x7fffffe120 --> 0x7fffffe150 --> 0x7fffffe340 (--> ...)
RSP: 0x7fffffc8d0 --> 0x0
RIP: 0x7ffff6e41e97 (<__GI_raise+199>: mov rcx,QWORD PTR [rsp+0x108])
R8 : 0x0
R9 : 0x7fffffc8d0 --> 0x0
R10: 0x8
R11: 0x246
R12: 0x7fffffd890 --> 0x7fffffd8d0 --> 0x7fffffe120 --> 0x7fffffe150 --> 0x7fffffe340 --> 0x4f3870 (<__libc_csu_init>: push r15)
R13: 0x7fffffd888 --> 0x7fff00000070
R14: 0x7fffffd830 --> 0x6190000001ef --> 0x3e00070002000000
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| 0x7fffffc8d0 --> 0x0
0008| 0x7fffffc8d8 --> 0x7fffffe118 --> 0x0
0016| 0x7fffffc8e0 --> 0x3200b5ff
0024| 0x7fffffc8e8 --> 0x0
0032| 0x7fffffc8f0 --> 0x0
0040| 0x7fffffc8f8 --> 0x0
0048| 0x7fffffc900 --> 0x0
0056| 0x7fffffc908 --> 0x0
[-----]
Legend: code, data, rodata, value
Stopped reason: SIGABRT
__GI_raise (sig=1@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=1@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1 0x00007ffff6e43801 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 0x0000000004c2b5b in ttUSHORT (p=0x6190000004dc "") at ./SRC/stb_truetype.h:1254
#8 0x0000000004e13c1 in stbtt_InitFont_internal (info=0x7fffffe180, data=0x619000000080 "OTTO", fontstart=0x0)
   at ./SRC/stb_truetype.h:1422
#9 0x0000000004d71a3 in stbtt_InitFont (info=0x7fffffe180, data=0x619000000080 "OTTO", offset=0x0)
   at ./SRC/stb_truetype.h:4771
#10 0x0000000004e1b29 in main (argc=0x2, argv=0x7fffffe428) at ../fuzzsrc/ttfuzz.c:29
#11 0x00007ffff6e24b97 in __libc_start_main (main=0x4e18f0 <main>, argc=0x2, argv=0x7fffffe428,
   init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffe418)
   at ../csu/libc-start.c:310
#12 0x00000000041ad4a in _start ()
```

carnil commented on Jan 10, 2020


[CVE-2020-6621](#) 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

