New issue

Jump to bottom

heap-use-after-free exists in the function grow_unicode in /lib/ttf.c #190

Open **Freewind9** opened this issue on Jul 28 · 0 comments

Freewind9 commented on Jul 28 • edited

system info
Ubuntu x86_64, clang 10.0, ttftool (latest master 772e55a)

Command line
./src/ttftool poc

```
=================================================================
==26408==ERROR: AddressSanitizer: heap-use-after-free on address 0x60300000017c at pc
0x0000004942df bp 0x7ffdd79c0b40 sp 0x7ffdd79c0308
WRITE of size 48 at 0x60300000017c thread T0
    #0 0x4942de in __asan_memset (/project/models/swftools/src/ttftool+0x4942de)
    #1 0x4cd29a in memset /usr/include/x86_64-linux-gnu/bits/string_fortified.h:71:10
    #2 0x4cd29a in grow_unicode /project/models/swftools/lib/ttf.c:1235:2
    #3 0x4cd29a in cmap_parse /project/models/swftools/lib/ttf.c:1283:6
    #4 0x4eb056 in ttf_parse_tables /project/models/swftools/lib/ttf.c:1901:2
    #5 0x4eb056 in ttf_load /project/models/swftools/lib/ttf.c:2180:9
    #6 0x51054c in ttf_open /project/models/swftools/lib/ttf.c:2435:17
    #7 0x4c51da in main /project/models/swftools/src/ttftool.c:91:19
    #8 0x7fe8b7a25082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
    #9 0x41c43d in _start (/project/models/swftools/src/ttftool+0x41c43d)

0x60300000017c is located 0 bytes to the right of 28-byte region [0x603000000160,0x60300000017c)
freed by thread T0 here:
    #0 0x494e99 in realloc (/project/models/swftools/src/ttftool+0x494e99)
    #1 0x517e2d in rfx_realloc /project/models/swftools/lib/mem.c:50:11

previously allocated by thread T0 here:
    #0 0x494cf2 in calloc (/project/models/swftools/src/ttftool+0x494cf2)
    #1 0x518011 in rfx_calloc /project/models/swftools/lib/mem.c:69:9

SUMMARY: AddressSanitizer: heap-use-after-free (/project/models/swftools/src/ttftool+0x4942de) in
__asan_memset
Shadow bytes around the buggy address:
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff8000: fa fa 00 00 00 04 fa fa 00 00 00 06 fa fa fd fd
  0x0c067fff8010: fd fa fa fa fd fd fd fd fa fa 00 00 02 fa fa fa
=>0x0c067fff8020: 00 00 00 02 fa fa fd fd fd fd fa fa fd fd fd[fd]
  0x0c067fff8030: fa fa 00 00 00 04 fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8070: 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
==26408==ABORTING
```

poc

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant