matthiaskramm / swftools Public

Code · Issues 117 · Pull requests 5 · Actions · Projects · Wiki · ...

New issue

Jump to bottom

heap-buffer-overflow exists in the function readU8 in lib/ttf.c #188

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

```
=================================================================
==26368==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000086 at pc
0x0000004edfd2 bp 0x7ffe607a9f10 sp 0x7ffe607a9f08
READ of size 1 at 0x603000000086 thread T0
    #0 0x4edfd1 in readU8 /project/models/swftools/lib/ttf.c:83:12
    #1 0x4edfd1 in os2_parse /project/models/swftools/lib/ttf.c:467:30
    #2 0x4edfd1 in ttf_parse_tables /project/models/swftools/lib/ttf.c:1849:13
    #3 0x4edfd1 in ttf_load /project/models/swftools/lib/ttf.c:2180:9
    #4 0x51054c in ttf_open /project/models/swftools/lib/ttf.c:2435:17
    #5 0x4c51da in main /project/models/swftools/src/ttftool.c:91:19
    #6 0x7f84d73a1082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
    #7 0x41c43d in _start (/project/models/swftools/src/ttftool+0x41c43d)

0x603000000086 is located 0 bytes to the right of 22-byte region [0x603000000070,0x603000000086)
allocated by thread T0 here:
    #0 0x494b7d in malloc (/project/models/swftools/src/ttftool+0x494b7d)
    #1 0x4e083a in ttf_load /project/models/swftools/lib/ttf.c:2160:15
    #2 0x51054c in ttf_open /project/models/swftools/lib/ttf.c:2435:17
    #3 0x7f84d73a1082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082)

SUMMARY: AddressSanitizer: heap-buffer-overflow /project/models/swftools/lib/ttf.c:83:12 in readU8
Shadow bytes around the buggy address:
  0x0c067fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  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 00 00
=>0x0c067fff8010:[06]fa fa fa 00 00 06 fa fa fa fd fd fd fd fa fa
```

```
  0x0c067fff8020: 00 00 02 fa fa fa 00 00 00 02 fa fa fa fa fa fa
  0x0c067fff8030: fa fa fa fa fa fa 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
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
==26368==ABORTING
```

poc

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant