LibreDWG / **libredwg** Public

<> Code ⊙ **Issues** 60 Pull requests Discussions Actions Security ···

New issue

Jump to bottom

A heap buffer overflow in appinfo_private at decode.c:2993 #252

Closed **seviezhou** opened this issue on Jul 31, 2020 · 0 comments

Assignees

Labels bug fuzzing

Milestone 0.11

seviezhou commented on Jul 31, 2020

System info:

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), dwg2dxf (latest master aee0ea)

Command line

./programs/dwg2dxf -b -m ./heap-buffer-overflow-appinfo_private-decode-2993 -o /dev/null

AddressSanitizer output

```
Reading DWG file ./heap-buffer-overflow-appinfo_private-decode-2993
=================================================================
==50338==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000c436 at pc 0x7f19fcaa3676 bp 0x7ffc0845d750 sp 0x7ffc0845cef8
READ of size 12 at 0x60200000c436 thread T0
    #0 0x7f19fcaa3675 in __interceptor_memcmp (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x77675)
    #1 0x56136d532338 in appinfo_private /home/seviezhou/libredwg/src/decode.c:2993
    #2 0x56136d532338 in read_2004_section_appinfo /home/seviezhou/libredwg/src/decode.c:3023
    #3 0x56136d532338 in decode_R2004 /home/seviezhou/libredwg/src/decode.c:3675
    #4 0x56136d53e3db in dwg_decode /home/seviezhou/libredwg/src/decode.c:242
    #5 0x56136d4391fc in dwg_read_file /home/seviezhou/libredwg/src/dwg.c:251
    #6 0x56136d436594 in main /home/seviezhou/libredwg/programs/dwg2dxf.c:258
    #7 0x7f19fc2beb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x56136d437689 in _start (/home/seviezhou/libredwg/programs/dwg2dxf+0xa4b689)

0x60200000c436 is located 0 bytes to the right of 6-byte region [0x60200000c430,0x60200000c436)
allocated by thread T0 here:
    #0 0x7f19fcac4612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
    #1 0x56136d47a234 in bit_read_TU16 /home/seviezhou/libredwg/src/bits.c:1878
    #2 0x29d  (<unknown module>)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __interceptor_memcmp
Shadow bytes around the buggy address:
  0x0c047fff9830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9840: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9850: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9860: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9870: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c047fff9880: fa fa fa fa fa fa[06]fa fa fa 04 fa fa fa 00 fa
  0x0c047fff9890: fa fa 00 fa fa fa 00 fa fa fa 04 fa fa fa 00 fa
  0x0c047fff98a0: fa fa 04 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0c047fff98b0: fa fa 02 fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0c047fff98c0: fa fa 00 fa fa fa 00 06 fa fa 00 fa fa fa 00 fa
  0x0c047fff98d0: fa fa 00 fa fa fa 00 fa fa fa 00 00 fa fa 00 02
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==50338==ABORTING
```

POC

heap-buffer-overflow-appinfo_private-decode-2993.zip

rurban self-assigned this on Jul 31, 2020

rurban added bug fuzzing labels on Jul 31, 2020

rurban added this to the **0.11** milestone on Jul 31, 2020

rurban added a commit that referenced this issue on Jul 31, 2020

`decode: improve appinfo is_teigha check` … 966beb5

rurban closed this as completed on Aug 1, 2020

Assignees

rurban

Labels

bug fuzzing

Projects

None yet

Milestone

0.11

Development

No branches or pull requests

2 participants