

New issue

Jump to bottom

A Segmentation fault in bits.c:186 #262

Closed seviezhou opened this issue on Aug 3, 2020 · 2 comments

Assignees



Labels

bug fuzzing

Milestone

0.11

seviezhou commented on Aug 3, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), dwg2dxf (latest master [bacd017](#))

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

Command line

./programs/dwg2dxf -b -m ./SEGV-bit_read_BB-bits-186 -o /dev/null

Output

Segmentation fault (core dumped)

AddressSanitizer output

```
ASAN:SIGSEGV
=====
==33413==ERROR: AddressSanitizer: SEGV on unknown address 0x63001e0dec1 (pc 0x56001ae1aa1c bp 0x7ffc0f008820 sp 0x7ffc0f008570 T0)
#0 0x56001ae1aa1b in bit_read_BB /home/seviezhou/libredwg/src/bits.c:186
#1 0x56001ae3d11b in bit_read_BS /home/seviezhou/libredwg/src/bits.c:525
#2 0x56001ae3d11b in bit_read_TU /home/seviezhou/libredwg/src/bits.c:1891
#3 0x56001ae4d52b in bit_read_CMC /home/seviezhou/libredwg/src/bits.c:2610
#4 0x56001a5261c2 in dwg_decode_VIEWPORT_private /home/seviezhou/libredwg/src/dwg.spec:1674
#5 0x56001aef02ff in dwg_decode_VIEWPORT /home/seviezhou/libredwg/src/dwg.spec:1607
#6 0x56001aef02ff in dwg_decode_add_object /home/seviezhou/libredwg/src/decode.c:5583
#7 0x56001aef77b8 in read_2004_section_handles /home/seviezhou/libredwg/src/decode.c:2843
#8 0x56001aef77b8 in decode_R2004 /home/seviezhou/libredwg/src/decode.c:3682
#9 0x56001af060ba in dwg_decode /home/seviezhou/libredwg/src/decode.c:242
#10 0x56001adfc094 in dwg_read_file /home/seviezhou/libredwg/src/dwg.c:251
#11 0x56001adfa242 in main /home/seviezhou/libredwg/programs/dwg2dxf.c:258
#12 0x7f13152a8b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#13 0x56001adfb2b9 in _start (/home/seviezhou/libredwg/programs/dwg2dxf+0xa8d2b9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/libredwg/src/bits.c:186 bit_read_BB
==33413==ABORTING
```

POC

[SEGV-bit_read_BB-bits-186.zip](#)

rurban self-assigned this on Aug 4, 2020

rurban commented on Aug 4, 2020

Contributor

The root cause is wrong error handling of obj_string_stream overflow (illegal str_dat stream bounds)


rurban added a commit that referenced this issue on Aug 4, 2020

decode: fix obj_string_stream overflow handling ...

092725e

rurban added this to the 0.11 milestone on Aug 4, 2020

rurban added bug fuzzing labels on Aug 4, 2020

 **rurban** added a commit that referenced this issue on Aug 4, 2020

 decode: fix obj_string_stream overflow handling ...

 66a3484

rurban commented on Aug 4, 2020

Contributor

Fixed with [66a3484](#)

 **rurban** closed this as completed on Aug 4, 2020

Assignees

 **rurban**

Labels

bug **fuzzing**

Projects

None yet

Milestone

0.11

Development

No branches or pull requests

2 participants