New issue

Jump to bottom

A Segmentation fault error in check_POLYLINE_handles at decode.c:5110 #251

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 ./SEGV-check_POLYLINE_handles-decode-5110 -o /dev/null

Output

```
Reading DWG file ./crashes/SEGV-check_POLYLINE_handles-decode-5110
Warning: checksum: 0x28751255 (calculated) mismatch

ERROR: Invalid EED size 59410 > 5
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
Warning: check_CRC mismatch 4410-4424 = 14: D8BC <=> C37B

Warning: Unstable Class object 504 TABLESTYLE (0xfff) 42/0
Warning: TODO TABLESTYLE r2010+ missing fields
Warning: Unstable Class object 505 MATERIAL (0x481) 45/0
Warning: Unstable Class object 505 MATERIAL (0x481) 46/0
Warning: Unstable Class object 505 MATERIAL (0x481) 47/0
ERROR: Invalid object handle 0.0.0 at pos @2.2
ERROR: bit_read_RC buffer overflow at 54
ERROR: bit_read_RC buffer overflow at 54
ERROR: bit_read_RC buffer overflow at 54
ERROR: bit_read_RC buffer overflow at 54
ERROR: bit_read_RC buffer overflow at 54
Warning: Wrong POLYLINE.layer 0
Warning: POLYLINE.layer is vertex[0] 10, shift em, NULL seqend
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==31426==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55638c2df408 bp 0x000000000004 sp 0x7ffd7da9bd40 T0)
    #0 0x55638c2df407 in check_POLYLINE_handles /home/seviezhou/libredwg/src/decode.c:5110
    #1 0x55638cd140de in dwg_decode_add_object /home/seviezhou/libredwg/src/decode.c:5514
    #2 0x55638cd20d90 in read_2004_section_handles /home/seviezhou/libredwg/src/decode.c:2835
    #3 0x55638cd20d90 in decode_R2004 /home/seviezhou/libredwg/src/decode.c:3671
    #4 0x55638cd2f3db in dwg_decode /home/seviezhou/libredwg/src/decode.c:242
    #5 0x55638cc2a1fc in dwg_read_file /home/seviezhou/libredwg/src/dwg.c:251
    #6 0x55638cc27594 in main /home/seviezhou/libredwg/programs/dwg2dxf.c:258
    #7 0x7f8cf6f20b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x55638cc28689 in _start (/home/seviezhou/libredwg/programs/dwg2dxf+0xa4b689)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/libredwg/src/decode.c:5110 check_POLYLINE_handles
==31426==ABORTING
```

POC

SEGV-check_POLYLINE_handles-decode-5110.zip

rurban added bug fuzzing labels on Jul 31, 2020

rurban self-assigned this 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: fix check_POLYLINE_handles NULL deref ... 8ebc76a

 **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