New issue

Jump to bottom

A double free in dwg.spec:7662 #256

Closed seviezhou opened this issue on Aug 1, 2020 · 1 comment

Assignees

Labels fuzzing

seviezhou commented on Aug 1, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), dwgbmp (latest master 4b99ed)

Configure

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

Command line

./programs/dwgbmp ./double-free-dwg_free_MATERIAL_private-dwg.spec-7662 /tmp/a.bmp

AddressSanitizer output

```
=================================================================
==29185==ERROR: AddressSanitizer: attempting double-free on 0x60c00000b140 in thread T0:
    #0 0x7ff7ab4c22da in free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x982da)
    #1 0x55bd65d40854 in dwg_free_MATERIAL_private /home/seviezhou/libredwg/src/dwg.spec:7662
    #2 0x55bd65dec9d4 in dwg_free_MATERIAL /home/seviezhou/libredwg/src/dwg.spec:7640
    #3 0x55bd65e6c14e in dwg_free_object /home/seviezhou/libredwg/src/free.c:862
    #4 0x55bd65e736fc in dwg_free /home/seviezhou/libredwg/src/free.c:1266
    #5 0x55bd65b897d7 in bmp_free_dwg /home/seviezhou/libredwg/programs/dwgbmp.c:95
    #6 0x55bd65b89e1b in get_bmp /home/seviezhou/libredwg/programs/dwgbmp.c:133
    #7 0x55bd65b88bca in main /home/seviezhou/libredwg/programs/dwgbmp.c:301
    #8 0x7ff7aacbcb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #9 0x55bd65b893e9 in _start (/home/seviezhou/libredwg/programs/dwgbmp+0x4e23e9)

0x60c00000b140 is located 0 bytes inside of 128-byte region [0x60c00000b140,0x60c00000b1c0)
freed by thread T0 here:
    #0 0x7ff7ab4c22da in free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x982da)
    #1 0x55bd657f449b in dwg_decode_MATERIAL_private /home/seviezhou/libredwg/src/dwg.spec:7665
    #2 0xb4  (<unknown module>)

previously allocated by thread T0 here:
    #0 0x7ff7ab4c27aa in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x987aa)
    #1 0x55bd657f2777 in dwg_decode_MATERIAL_private /home/seviezhou/libredwg/src/dwg.spec:7662
    #2 0xb4  (<unknown module>)

SUMMARY: AddressSanitizer: double-free ??:0 free
==29185==ABORTING
```

POC

double-free-dwg_free_MATERIAL_private-dwg.spec-7662.zip

rurban added the fuzzing label on Aug 1, 2020

rurban self-assigned this on Aug 1, 2020

rurban added a commit that referenced this issue on Aug 1, 2020

spec: fix MATERIAL.map ... 34df8ca

rurban commented on Aug 1, 2020 Contributor

Excellent find!
The spec was wrong here.

rurban added a commit that referenced this issue on Aug 1, 2020

spec: fix MATERIAL.map ... 8582ca9

rurban closed this as completed on Aug 1, 2020

Assignees

rurban

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants