New issue

Jump to bottom

NULL pointer deference #186

Closed **skyvast404** opened this issue on Jan 14, 2020 · 3 comments

Assignees

Labels fuzzing

Milestone 0.11

skyvast404 commented on Jan 14, 2020 • edited

Hello, I got a NULL pointer deference bug in **0.10.1.2677 and even earlier** by run `dxf2dwg poc -o /dev/null`

```
==12391==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f9f9b4f3284 bp 0x7ffcfa3b08a0 sp 0x7ffcfa3b0860 T0)
==12391==The signal is caused by a READ memory access.
==12391==Hint: address points to the zero page.
    #0 0x7f9f9b4f3283 in add_MLINESTYLE_lines /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:1462
    #1 0x7f9f9b554a23 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:5897
    #2 0x7f9f9b564d2d in dxf_objects_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7245
    #3 0x7f9f9b56bb16 in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7701
    #4 0x7f9f9a684ee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
    #5 0x564a81d20465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
    #6 0x7f9f99d8fb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x564a81d1f489 in _start (/home/skyvast/Documents/asan_libredwg/bin/dxf2dwg+0x2489)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:1462 in add_MLINESTYLE_lines
==12391==ABORTING
```

rurban self-assigned this on Jan 14, 2020

rurban commented on Jan 14, 2020 Contributor

Can you attach the poc please?

rurban added a commit that referenced this issue on Jan 14, 2020

`indxf: more NULL pair protections` ... a53e2e3

rurban added this to the **0.11** milestone on Jan 14, 2020

skyvast404 commented on Jan 15, 2020 Author

null_pointer.zip

rurban added the fuzzing label on Jan 16, 2020

rurban added a commit that referenced this issue on Jan 16, 2020

`indxf: fix 3x NULL pair SEGV` ... acaecee

rurban closed this as completed on Jan 16, 2020

skyvast404 commented on Jul 19, 2020 Author

This bug credited by ADLab.
CVE-2020-15807

DavidKorczynski mentioned this issue on Feb 23, 2021

libredwg: initial integration. google/oss-fuzz#5226

Merged

Assignees

rurban

Labels

fuzzing

Projects

None yet

Milestone

0.11

Development

No branches or pull requests

2 participants