New issue

Jump to bottom

heap-use-after-free exists in the function dwg_add_handleref in dwg.c #490

Open **cxlzff** opened this issue on Jun 6 · 2 comments

Assignees

Labels bug fuzzing invalid CVE

cxlzff commented on Jun 6

system info

Ubuntu x86_64, clang 6.0, dwg2dxf(0.12.4.4608)

Command line

./programs/dwg2dxf -b -m @@ -o /dev/null

AddressSanitizer output

==8997==ERROR: AddressSanitizer: heap-use-after-free on address 0x604000000730 at pc 0x000000517369 bp 0x7fffffffc7d0 sp 0x7fffffffc7c8
READ of size 8 at 0x604000000730 thread T0
#0 0x517368 in dwg_add_handleref /testcase/libredwg/src/dwg.c:2014:21
#1 0x7ea615 in dwg_add_BLOCK_HEADER /testcase/libredwg/src/dwg_api.c:24588:3
#2 0x70baf6 in decode_preR13_section /testcase/libredwg/src/decode_r11.c:325:20
#3 0x705d0a in decode_preR13 /testcase/libredwg/src/decode_r11.c:830:12
#4 0x53245a in dwg_decode /testcase/libredwg/src/decode.c:209:23
#5 0x50d759 in dwg_read_file /testcase/libredwg/src/dwg.c:254:11
#6 0x50c454 in main /testcase/libredwg/programs/dwg2dxf.c:258:15
#7 0x7ffff6e22c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#8 0x419ee9 in _start (/testcase/libredwg/programs/dwg2dxf+0x419ee9)

0x604000000730 is located 32 bytes inside of 48-byte region [0x604000000710,0x604000000740)
freed by thread T0 here:
#0 0x4d23a0 in __interceptor_cfree.localalias.0 /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:55
#1 0x7070a2 in decode_preR13_header_variables /testcase/libredwg/src/./header_variables_r11.spec:65:3
#2 0x232900001100144d ()

previously allocated by thread T0 here:
#0 0x4d2750 in calloc /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:74
#1 0x54900c in dwg_new_ref /testcase/libredwg/src/decode.c:4027:43

SUMMARY: AddressSanitizer: heap-use-after-free /testcase/libredwg/src/dwg.c:2014:21 in dwg_add_handleref
Shadow bytes around the buggy address:
0x0c087fff8090: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 fa
0x0c087fff80a0: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff80b0: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff80c0: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff80d0: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
=>0x0c087fff80e0: fa fa fd fd fd fd[fd]fd fa fa 00 00 00 00 00 00
0x0c087fff80f0: fa fa 00 00 00 00 00 00 fa fa fd fd fd fd fd fd
0x0c087fff8100: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff8110: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff8120: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
0x0c087fff8130: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
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
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
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
Left alloca redzone: ca
Right alloca redzone: cb
==8997==ABORTING

poc

https://gitee.com/cxlzff/fuzz-poc/raw/master/libredwg/dwg_add_handleref_uaf

rurban added bug **fuzzing** labels on Jun 7

rurban self-assigned this on Jun 7

abergmann commented on Jun 24

CVE-2022-33027 was assigned to this issue.

rurban commented on Jun 24 Contributor

Invalid CVE, not repro in the latest release 0.12.5.

The tested version is experimental and preR13 DWG's lead to:

```
Reading DWG file ../test/issues/gh490/dwg_add_handleref_uaf
ERROR: This version of LibreDWG is only capable of decoding version r13-r2018 (code: AC1012-
AC1032) DWG files.
We don't decode many entities and no blocks yet.
ERROR: DWG too small 1338
ERROR: Failed to decode file: ../test/issues/gh490/dwg_add_handleref_uaf 0x800
```

rurban added the **invalid CVE** label on Jun 24

Assignees

rurban

Labels

bug **fuzzing** **invalid CVE**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

3 participants