LibreDWG / **libredwg** Public

Code · Issues 77 · Pull requests 2 · Discussions · Actions · Security · ...

New issue

Jump to bottom

heap-buffer-overflow exists in the function dwg_add_object in decode.c #489

○ 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

```
==8995==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62e00000ac80 at pc
0x0000004bc125 bp 0x7fffffffc7c0 sp 0x7fffffffbf70
WRITE of size 168 at 0x62e00000ac80 thread T0
#0 0x4bc124 in __asan_memset /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-
rt/lib/asan/asan_interceptors.cc:457
#1 0x5a062e in dwg_add_object /testcase/libredwg/src/decode.c:4740:3
#2 0x7e0942 in dwg_add_VIEW /testcase/libredwg/src/dwg_api.c:24619:3
#3 0x70c71e in decode_preR13_section /testcase/libredwg/src/decode_r11.c:434:13
#4 0x705d7a in decode_preR13 /testcase/libredwg/src/decode_r11.c:834:12
#5 0x53245a in dwg_decode /testcase/libredwg/src/decode.c:209:23
#6 0x50d759 in dwg_read_file /testcase/libredwg/src/dwg.c:254:11
#7 0x50c454 in main /testcase/libredwg/programs/dwg2dxf.c:258:15
#8 0x7ffff6e22c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#9 0x419ee9 in _start (/testcase/libredwg/programs/dwg2dxf+0x419ee9)
```

```
0x62e00000ac80 is located 0 bytes to the right of 43136-byte region [0x62e000000400,0x62e00000ac80)
allocated by thread T0 here:
#0 0x4d2968 in realloc /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:79
#1 0x70b9ca in decode_preR13_section /testcase/libredwg/src/decode_r11.c:273:32
#2 0x705d7a in decode_preR13 /testcase/libredwg/src/decode_r11.c:834:12
#3 0x50d759 in dwg_read_file /testcase/libredwg/src/dwg.c:254:11
#4 0x50c454 in main /testcase/libredwg/programs/dwg2dxf.c:258:15
#5 0x7ffff6e22c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-rt/lib/asan/asan_interceptors.cc:457 in __asan_memset
Shadow bytes around the buggy address:
0x0c5c7fff9540: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c5c7fff9550: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c5c7fff9560: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c5c7fff9570: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c5c7fff9580: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5c7fff9590:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c5c7fff95a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c5c7fff95b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c5c7fff95c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c5c7fff95d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c5c7fff95e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==8995==ABORTING
```

poc

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

rurban added bug fuzzing labels on Jun 7

rurban self-assigned this on Jun 7

abergmann commented on Jun 24

CVE-2022-33028 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/gh489/dwg_add_object_bof
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 1390
ERROR: Failed to decode file: ../test/issues/gh489/dwg_add_object_bof 0x800

READ ERROR 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