New issue   Jump to bottom

double-free exists in the function dwg_read_file in dwg.c #493

⊙ Open   cxlzff opened this issue on Jun 7 · 2 comments

Assignees

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

---

cxlzff commented on Jun 7

system info

Ubuntu x86_64, clang 6.0, dwg2dxf(0.12.4.4608)

Command line

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

AddressSanitizer output

==9541==ERROR: AddressSanitizer: attempting double-free on 0x61a000000100 in thread T0:
#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 0x50d77a in dwg_read_file /testcase/libredwg/src/dwg.c:258:7
#2 0x50c454 in main /testcase/libredwg/programs/dwg2dxf.c:258:15
#3 0x7ffff6e22c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#4 0x419ee9 in _start (/testcase/libredwg/programs/dwg2dxf+0x419ee9)

0x61a000000100 is located 128 bytes inside of 1321-byte region [0x61a000000080,0x61a0000005a9)
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 0x50cdd0 in dat_read_file /testcase/libredwg/src/dwg.c:91:33
#2 0x50d708 in dwg_read_file /testcase/libredwg/src/dwg.c:247:15
#3 0x50c454 in main /testcase/libredwg/programs/dwg2dxf.c:258:15
#4 0x7ffff6e22c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: double-free /fuzzer/build/llvm_tools/llvm-4.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:55 in __interceptor_cfree.localalias.0
==9541==ABORTING

poc

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

---

rurban added   bug   **fuzzing**   labels on Jun 8

rurban self-assigned this on Jun 8

abergmann commented on Jun 24

CVE-2022-33033 was assigned to this issue.

rurban commented on Jun 24   (Contributor)

Invalid CVE,
Not repro in the latest release 0.12.5:

```
Reading DWG file ../test/issues/gh493/dwg_read_file_df
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 1320
ERROR: Failed to decode file: ../test/issues/gh493/dwg_read_file_df 0x800
```

---

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

Assignees

  rurban

Labels

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

Projects

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

3 participants