

[New issue](#)[Jump to bottom](#)

heap-buffer-overflow exists in the function decode_preR13_section_hdr in decode_r11.c #488

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

```
==8993==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000000144 at pc
0x00000007064dc bp 0x7ffffffca00 sp 0x7ffffffc9f8
WRITE of size 4 at 0x611000000144 thread T0
#0 0x7064db in decode_preR13_section_hdr /testcase/libredwg/src/decode_r11.c:136:13
#1 0x70583b in decode_preR13 /testcase/libredwg/src/decode_r11.c:737:12
#2 0x53245a in dwg_decode /testcase/libredwg/src/decode.c:209:23
#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
#6 0x419ee9 in _start (/testcase/libredwg/programs/dwg2dxf+0x419ee9)
```

0x611000000144 is located 4 bytes to the right of 256-byte region [0x611000000040,0x611000000140) 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 0x7055f0 in decode_preR13 /testcase/libredwg/src/decode_r11.c:700:40

#2 0x50d759 in dwg_read_file /testcase/libredwg/src/dwg.c:254:11

#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: heap-buffer-overflow /testcase/libredwg/src/decode_r11.c:136:13 in decode_preR13_section_hdr

Shadow bytes around the buggy address:

0x0c227fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c227fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c227fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c227fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00

0x0c227fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

=>0x0c227fff8020: 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa

0x0c227fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c227fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c227fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c227fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c227fff8070: 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

==8993==ABORTING

poc

https://gitee.com/cxlzff/fuzz-poc/raw/master/libredwg/decode_preR13_section_hdr_bof

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

  **rurban** self-assigned this on Jun 7

abergmann commented on Jun 24

[CVE-2022-33032](#) 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 this preR13 DWG leads to:

```
Reading DWG file ../test/issues/gh488/decode_preR13_section_hdr_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: Invalid table number 1845522176 for UCS      [ 7]
ERROR: Invalid table number 6619244 for VPORTRT    [ 8]
ERROR: Invalid table number 2228275 for APPID      [ 9]
ERROR: Invalid table number 341118858 for VX       [11]
ERROR: Failed to decode file: ../test/issues/gh488/decode_preR13_section_hdr_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

