

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

heap-buffer-overflow exists in the function bit_calc_CRC in bits.c #484

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

```
==8982==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000592 at pc
0x00000005289e1 bp 0x7ffffffca80 sp 0x7ffffffca78
READ of size 1 at 0x616000000592 thread T0
#0 0x5289e0 in bit_calc_CRC /testcase/libredwg/src/bits.c:3257:29
#1 0x7059b1 in decode_preR13 /testcase/libredwg/src/decode_r11.c:760:14
#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)
```

0x616000000592 is located 0 bytes to the right of 530-byte region [0x616000000380,0x616000000592) 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: heap-buffer-overflow /testcase/libredwg/src/bits.c:3257:29 in bit_calc_CRC
Shadow bytes around the buggy address:

0x0c2c7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c2c7fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c2c7fff8090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c2c7fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff80b0: 00 00[02]fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c2c7fff8100: 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

==8982==ABORTING

poc

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

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

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

abergmann commented on Jun 24

[CVE-2022-33026](#) 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/gh484/bit_calc_CRC_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 529
ERROR: Failed to decode file: ../test/issues/gh484/bit_calc_CRC_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

