# Heap overflow due to incomplete fix for issues #255 #258

Closed seviezhou opened this issue on Aug 1, 2020 · 0 comments

Assignees

Labels bug fuzzing

Milestone 0.11

seviezhou commented on Aug 1, 2020

## System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), dwgbmp (latest master 39ef943)

## Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

## Command line

./programs/dwgbmp ./heap-overflow-bit_wcs2nlen-bit-1636

## AddressSanitizer output

```
=================================================================
==23940==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61600000ec80 at pc 0x558b22fdc723 bp 0x7ffe585f6d40 sp 0x7ffe585f6d30
READ of size 2 at 0x61600000ec80 thread T0
    #0 0x558b22fdc722 in bit_wcs2nlen /home/seviezhou/libredwg/src/bits.c:1636
    #1 0x558b22c13540 in dwg_decode_LTYPE_private /home/seviezhou/libredwg/src/dwg.spec:3020
    #2 0x558b2308fb8d in dwg_decode_LTYPE /home/seviezhou/libredwg/src/dwg.spec:2936
    #3 0x558b2308fb8d in dwg_decode_add_object /home/seviezhou/libredwg/src/decode.c:5669
    #4 0x558b23097a03 in read_2004_section_handles /home/seviezhou/libredwg/src/decode.c:2843
    #5 0x558b23097a03 in decode_R2004 /home/seviezhou/libredwg/src/decode.c:3680
    #6 0x558b230a5a36 in dwg_decode /home/seviezhou/libredwg/src/decode.c:242
    #7 0x558b22f9edec in dwg_read_file /home/seviezhou/libredwg/src/dwg.c:251
    #8 0x558b22f9ce28 in get_bmp /home/seviezhou/libredwg/programs/dwgbmp.c:120
    #9 0x558b22f9bed0 in main /home/seviezhou/libredwg/programs/dwgbmp.c:301
    #10 0x7f0a4446eb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #11 0x558b22f9c6a9 in _start (/home/seviezhou/libredwg/programs/dwgbmp+0x4e76a9)

0x61600000ec81 is located 0 bytes to the right of 513-byte region [0x61600000ea80,0x61600000ec81)
allocated by thread T0 here:
    #0 0x7f0a44c747aa in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x987aa)
    #1 0x558b22fd7de8 in bit_read_TF /home/seviezhou/libredwg/src/bits.c:1444

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/libredwg/src/bits.c:1636 bit_wcs2nlen
Shadow bytes around the buggy address:
  0x0c2c7fff9d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff9d50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9d60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9d70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9d80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff9d90:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff9da0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff9db0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9dc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9dd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff9de0: 00 00 00 00 00 00 00 00 00 00 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==23940==ABORTING
```

## POC

heap-overflow-bit_wcs2nlen-bit-1636.zip

**seviezhou** changed the title ~~Incomplete fix for issues #255~~ **Heap overflow due to incomplete fix for issues #255** on Aug 1, 2020

**rurban** self-assigned this on Aug 2, 2020

**rurban** added bug fuzzing labels on Aug 2, 2020

**rurban** added this to the **0.11** milestone on Aug 2, 2020

**rurban** added a commit that referenced this issue on Aug 2, 2020

`fixup LTYPE.dashes overflows` … ✕ `dac8fcc`

**rurban** closed this as completed on Aug 2, 2020

Assignees

rurban

Labels

bug fuzzing

Projects

None yet

Milestone

0.11

Development

No branches or pull requests

2 participants