

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

# stack-buffer-overflow exists in the function copy\_bytes in decode\_r2007.c #494

Open cxlzzf opened this issue on Jun 7 · 2 comments

Assignees



Labels

[bug](#) [fuzzing](#)

cxlzzf 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

```
==9543==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffffffc8f0 at pc 0x0000007257bb
bp 0x7ffffffc90 sp 0x7ffffffc88
WRITE of size 1 at 0x7ffffffc8f0 thread T0
#0 0x7257ba in copy_bytes /testcase/libredwg/src/decode_r2007.c:228:12
#1 0x7257ba in decompress_r2007 /testcase/libredwg/src/decode_r2007.c:563
#2 0x712263 in read_file_header /testcase/libredwg/src/decode_r2007.c:1247:13
#3 0x712263 in read_r2007_meta_data /testcase/libredwg/src/decode_r2007.c:2354
#4 0x533116 in decode_R2007 /testcase/libredwg/src/decode.c:3231:11
#5 0x533116 in dwg_decode /testcase/libredwg/src/decode.c:212
#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)
```

Address 0x7ffffffc8f0 is located in stack of thread T0 at offset 2736 in frame  
#0 0x71159f in read\_r2007\_meta\_data /testcase/libredwg/src/decode\_r2007.c:2338

This frame has 23 object(s):

[32, 40) 'acis\_sab\_data.i.i'

[64, 65) 'acis\_empty.i.i'

[80, 82) 'version1913.i.i'

[96, 100) 'size1930.i.i'

[112, 160) 'sec\_dat.i548'

[192, 240) 'sec\_dat.i515'

[272, 320) 'sec\_dat.i492'

[352, 400) 'sec\_dat.i455'

[432, 480) 'sec\_dat.i424'

[512, 560) 'sec\_dat.i391'

[592, 640) 'sec\_dat.i356'

[672, 720) 'sec\_dat.i330'

[752, 800) 'sec\_dat.i301'

[832, 836) 'size.i282'

[848, 873) 'old\_dat.sroa.0.i'

[912, 960) 'sec\_dat.i268'

[992, 1040) 'sec\_dat.i220'

[1072, 1120) 'str.i'

[1152, 1200) 'sec\_dat.i'

[1232, 1280) 'str\_dat.i'

[1312, 1320) 'ptr.i'

[1344, 2328) 'data.i'

[2464, 2736) 'file\_header' <== Memory access at offset 2736 overflows this variable

HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext

(longjmp and C++ exceptions *are* supported)

SUMMARY: AddressSanitizer: stack-buffer-overflow /testcase/libredwg/src/decode\_r2007.c:228:12 in copy\_bytes

Shadow bytes around the buggy address:

0x10007fff78c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x10007fff78d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x10007fff78e0: 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2

0x10007fff78f0: f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 00 00 00 00

0x10007fff7900: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

=>0x10007fff7910: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [f3]f3

0x10007fff7920: f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00

0x10007fff7930: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x10007fff7940: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x10007fff7950: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x10007fff7960: 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

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  
==9543==ABORTING

**poc**

[https://gitee.com/cxlzff/fuzz-poc/raw/master/libredwg/copy\\_bytes\\_sof](https://gitee.com/cxlzff/fuzz-poc/raw/master/libredwg/copy_bytes_sof)

  **rurban** self-assigned this on Jun 8

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

**abergmann** commented on Jun 24


[CVE-2022-33034](#) was assigned to this issue.

**rurban** commented on Jun 24

Contributor

repro in v0.12.5, the latest release

#### Assignees

 **rurban**

#### Labels

**bug** **fuzzing**

#### Projects

projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

3 participants

