

New issue

Jump to bottom

Four NULL dereference in out_dxf.c #324

🔒 Closed zodf0055980 opened this issue on Mar 3, 2021 · 1 comment

Assignees



Labels

bug fuzzing

Milestone

🏠 0.12.4

zodf0055980 commented on Mar 3, 2021 • edited

I found four NULL dereference bugs in the current master ([5d2c75f](#)).

Configure

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

bug 1 in out_dxf.c:1902

Command

```
./dwg2dxf -o ./fuzz_out -b -y ./poc1
```

ASAN report

```
→ ./dwg2dxf -o ./fuzz_out -b -y ./poc1
Reading DWG file ./poc1
Warning: checksum: 0x27c51243 (calculated) mismatch

ERROR: Skip section AcDb:FileDepList with size 8 > 0 * 128
ERROR: obj_string_stream overflow, bitsize 96 => 96
ERROR: Invalid object handle 10.1.1 at pos @4.2
ERROR: bit_read_RC buffer overflow at 12
ERROR: bit_read_RC buffer overflow at 12
ERROR: bit_read_RC buffer overflow at 12
ERROR: bit_read_RC buffer overflow at 12 >= 12
ERROR: bit_read_BL: unexpected 2-bit code: '11'
ERROR: bit_read_RC buffer overflow at 12
ERROR: Invalid CMC method 0x0 ignored
ERROR: bit_advance_position buffer overflow at pos 11.7, size 12, advance by 2
ERROR: bit_read_BD buffer overflow at 12 >= 12
ERROR: Invalid BD identifier_height
Warning: check_CRC mismatch 22-38 = 16: 401C <=> 0B9D

Warning: Unstable Class object 502 TABLESTYLE (0xffff) 42/0
Warning: TODO TABLESTYLE r2010+ missing fields
Warning: Unstable Class object 503 MATERIAL (0x481) 45/0
Warning: Unstable Class object 503 MATERIAL (0x481) 46/0
Warning: Unstable Class object 503 MATERIAL (0x481) 47/0
Warning: Ignore invalid handleoff (@390)
ERROR: bit_read_RC buffer overflow at 174
ERROR: bit_read_RC buffer overflow at 171
ERROR: bit_read_RC buffer overflow at 973
ERROR: bit_read_RC buffer overflow at 284
ERROR: bit_read_RC buffer overflow at 284
ERROR: Some section size or address out of bounds
ERROR: Failed to read uncompressed Preview section
Warning: Skip empty section 0 AcDb:Template
ERROR: Template section not found

ERROR: Invalid num_segidx
Warning: Object handle not found, 2/2 in 150 objects
Warning: Object handle not found, 2/2 in 150 objects
Warning: Object handle not found, 2/2 in 150 objects
Writing DXF file ./fuzz_out as r14
ASAN:DEADLYSIGNAL
=====
==17991==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x7ffff4cf2b1b bp 0x7fffffc9c0 sp 0x7fffff8450 T0)
==17991==The signal is caused by a READ memory access.
==17991==Hint: address points to the zero page.
#0 0x7ffff4cf2b1a in dxf_tables_write /home/yuan/af1-target/libredwg-asan/src/out_dxf.c:1902
#1 0x7ffff4d06d16 in dwg_write_dxf /home/yuan/af1-target/libredwg-asan/src/out_dxf.c:2312
#2 0x5555555589a1 in main /home/yuan/af1-target/libredwg-asan/programs/dwg2dxf.c:336
#3 0x7ffff1e6bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#4 0x555555556a89 in _start (/home/yuan/af1-target/libredwg-asan/programs/.libs/dwg2dxf+0x2a89)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yuan/af1-target/libredwg-asan/src/out_dxf.c:1902 in dxf_tables_write
==17991==ABORTING
```

bug 2 in out_dxf.c:1924

Command

```
./dwg2dxf -o ./fuzz_out -b -y ./poc2
```

ASAN report

```
→ ./dwg2dxf -o ./fuzz_out -b -y ./poc2
Reading DWG file ./poc2
Warning: checksum: 0x27c51243 (calculated) mismatch

ERROR: Skip section AcDb:FileDepList with size 8 > 0 * 128
ERROR: obj_string_stream overflow, bitsize 4294965675 => 88
ERROR: Invalid EED size 8770 > 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_read_RC buffer overflow at 11
ERROR: bit_advance_position buffer overflow at pos 10.7, size 11, advance by 2
ERROR: bit_read_BB buffer overflow at 11 >= 11
ERROR: bit_read_BD buffer overflow at 11 >= 11
ERROR: bit_read_B buffer overflow at 11 >= 11
ERROR: bit_read_BB buffer overflow at 11 >= 11
ERROR: bit_read_BD buffer overflow at 11 >= 11
ERROR: bit_read_RC buffer overflow at 11 >= 11
ERROR: bit_read_RD buffer overflow at 11 >= 11
ERROR: Invalid RD oblique_angle
Warning: check_CRC mismatch 39-54 = 15: C16F <=> 0D90

Warning: Unstable Class object 502 TABLESTYLE (0xffff) 42/0
Warning: TODO TABLESTYLE r2010+ missing fields
Warning: Unstable Class object 503 MATERIAL (0x481) 45/0
Warning: Unstable Class object 503 MATERIAL (0x481) 46/0
Warning: Unstable Class object 503 MATERIAL (0x481) 47/0
Warning: Ignore invalid handleoff (@390)
ERROR: bit_read_RC buffer overflow at 174
ERROR: bit_read_RC buffer overflow at 171
ERROR: bit_read_RC buffer overflow at 973
ERROR: bit_read_RC buffer overflow at 284
ERROR: bit_read_RC buffer overflow at 284
ERROR: Some section size or address out of bounds
ERROR: Failed to read uncompressed Preview section
Warning: Skip empty section 0 AcDb:Template
ERROR: Template section not found

ERROR: Invalid num_segidx
Warning: Object handle not found, 3/3 in 150 objects
Warning: Object handle not found, 3/3 in 150 objects
Warning: Object handle not found, 3/3 in 150 objects
Writing DXF file ./fuzz_out
ERROR: Unhandled VALUE_INT code 0
ASAN: DEADLYSIGNAL
=====
==18068==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x7ffff4cf4e7f bp 0x7fffffc9e0 sp 0x7fffffff8470 T0)
==18068==The signal is caused by a READ memory access.
==18068==Hint: address points to the zero page.
#0 0x7ffff4cf4e7e in dxf_tables_write /home/yuan/af1-target/libredwg-asan/src/out_dxfb.c:1924
#1 0x7ffff4d06d16 in dwg_write_dxfb /home/yuan/af1-target/libredwg-asan/src/out_dxfb.c:2312
#2 0x5555555589a1 in main /home/yuan/af1-target/libredwg-asan/programs/dwg2dxf.c:336
#3 0x7ffff1e6bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#4 0x555555556a89 in _start (/home/yuan/af1-target/libredwg-asan/programs/.libs/dwg2dxf+0x2a89)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yuan/af1-target/libredwg-asan/src/out_dxfb.c:1924 in dxf_tables_write
==18068==ABORTING
```

bug 3 in out_dxfb.c:1872

Command

```
./dwg2dxf -o ./fuzz_out -b -y poc3
```

ASAN report

```
→ ./dwg2dxf -o ./fuzz_out -b -y poc3
Reading DWG file poc3
Warning: checksum: 0x27c51243 (calculated) mismatch

ERROR: Skip section AcDb:FileDepList with size 8 > 0 * 128
ERROR: Invalid preview size 18496. Need min. 18496 bits for TF, have 76 for RAY.
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_RC buffer overflow at 13
ERROR: bit_read_BD buffer overflow at 13 >= 13
ERROR: bit_read_BB buffer overflow at 13 >= 13
```

```
Warning: Unstable Class object 502 TABLESTYLE (0xffff) 42/0
Warning: T000 TABLESTYLE r2010: missing fields
Warning: Unstable Class object 503 MATERIAL (0x481) 45/0
Warning: Unstable Class object 503 MATERIAL (0x481) 46/0
Warning: Unstable Class object 503 MATERIAL (0x481) 47/0
Warning: Ignore invalid handle0ff (@390)
ERROR: bit_read_RC buffer overflow at 174
ERROR: bit_read_RC buffer overflow at 171
ERROR: bit_read_RC buffer overflow at 973
ERROR: bit_read_RC buffer overflow at 284
ERROR: bit_read_RC buffer overflow at 284
ERROR: Some section size or address out of bounds
ERROR: Failed to read uncompressed Preview section
Warning: Skip empty section 0 ACdb:Template
ERROR: Template section not found
```

```
=====
--18124a--ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x7fffffc4968d bp 0x7fffffc9e8 sp 0x7fffffc8470 T0)
--18124a--The signal is caused by a READ memory access.
--18124a--Hint: address points to the zero page.
#0 0x7fffffc4968d in dxf_btables_write /home/yuan/af1-target/libredwg-asan/src/out_dxf.bc:1872
#1 0x7ffffc4d06d16 in dwg_write_dxf6 /home/yuan/af1-target/libredwg-asan/src/out_dxf.bc:2312
#2 0x5555555589a1 in main /home/yuan/af1-target/libredwg-asan/programs/dxf2dxf.c:336
#3 0x7ffffc16b6bf6 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6;0x21bf6)
#4 0x555555556a89 in _start (/home/yuan/af1-target/libredwg-asan/programs/_libs/dwg2dxf40x2a89)
```

bug 4 in out_dx.fb.c:1944

Command

ASAN report

[illegible]

```
Warning: Unstable Class object 502 TABLESTYLE (0xffff) 42/0
Warning: TODO TABLESTYLE r2080: missing fields
Warning: Unstable Class object 503 MATERIAL (0x481) 45/8
Warning: Unstable Class object 503 MATERIAL (0x481) 46/8
Warning: Unstable Class object 503 MATERIAL (0x481) 47/0
Warning: Ignore invalid handleoff (0390)
ERROR: bit_read_RC buffer overflow at 174
ERROR: bit_read_RC buffer overflow at 171
ERROR: bit_read_RC buffer overflow at 973
ERROR: bit_read_RC buffer overflow at 284
ERROR: bit_read_RC buffer overflow at 284
ERROR: Some section size or address out of bounds
ERROR: Failed to read uncompressed Preview section
Warning: Skip empty section 0 ACdb:Template
```

ERROR: Template section not found


```
ERROR: Invalid num_segidx
Writing DXF file ./fuzz_out as r12
ERROR: Unhandled VALUE_INT code 7
ASAN:DEADLYSIGNAL
=====
==18183==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x7ffff4cf71e3 bp 0x7ffffffc9c0 sp 0x7ffffff8450 T0)
==18183==The signal is caused by a READ memory access.
==18183==Hint: address points to the zero page.
#0 0x7ffff4cf71e2 in dxfb_tables_write /home/yuan/afl-target/libredwg-asan/src/out_dxfb.c:1944
#1 0x7ffff4d06d16 in dwg_write_dxfb /home/yuan/afl-target/libredwg-asan/src/out_dxfb.c:2312
#2 0x5555555589a1 in main /home/yuan/afl-target/libredwg-asan/programs/dwg2dxf.c:336
#3 0x7ffff1e6bbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#4 0x555555556a89 in _start (/home/yuan/afl-target/libredwg-asan/programs/.libs/dwg2dxf+0x2a89)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yuan/afl-target/libredwg-asan/src/out_dxfb.c:1944 in dxfb_tables_write
==18183==ABORTING
```

All poc

[poc.zip](#)

 **rurban** self-assigned this on Mar 3, 2021

  **rurban** added `bug` `fuzzing` labels on Mar 3, 2021

rurban commented on Mar 3, 2021

Contributor

--as r14 is not needed

 **rurban** added a commit that referenced this issue on Mar 3, 2021

 outdxfb: fix table NULL-derefs ...

6e92bae

  **rurban** added this to the **0.12.4** milestone on Mar 3, 2021

 **rurban** closed this as completed on Mar 3, 2021

Assignees

 **rurban**

Labels

`bug` `fuzzing`

Projects

None yet

Milestone

0.12.4

Development

No branches or pull requests

2 participants