

New issue

[Jump to bottom](#)

Assertion dwg2dxf: decode.c:5801: int
decode_preR13_entities(BITCODE_RL, BITCODE_RL, unsigned
int, BITCODE_RL, BITCODE_RL, Bit_Chain *, Dwg_Data *):
Assertion '!dat->bit' failed. Aborted. #492

 Open cxlzff opened this issue on Jun 6 · 3 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


output

dwg2dxf: decode.c:5801: int decode_preR13_entities(BITCODE_RL, BITCODE_RL, unsigned int, BITCODE_RL, BITCODE_RL, Bit_Chain *, Dwg_Data *): Assertion '!dat->bit' failed.
Aborted

poc

https://gitee.com/cxlzff/fuzz-poc/raw/master/libredwg/decode_preR13_entities_Assertion

  rurban added bug fuzzing labels on Jun 7

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

abergmann commented on Jun 24

[CVE-2022-33024](#) was assigned to this issue.

rurban commented on Jun 24

Contributor

Invalid CVE, not repro in the latest release 0.12.5

```
programs/dwg2dxf -b ../test/issues/gh492/decode_preR13_entities_Assertion
Reading DWG file ../test/issues/gh492/decode_preR13_entities_Assertion
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: Unknown object type 0
ERROR: Invalid table number 16 for LAYER [ 2]
ERROR: Invalid table number 65548 for STYLE [ 3]
ERROR: Invalid table number 128 for LTYPE [ 5]
ERROR: Invalid table number 67371008 for VIEW [ 6]
ERROR: Invalid table number -1643903996 for UCS [ 7]
ERROR: Invalid table number -457043299 for VPORT [ 8]
ERROR: Invalid table number -999567258 for APPID [ 9]
ERROR: Invalid table number -791621424 for DIMSTYLE [10]
ERROR: Invalid table number 67372036 for VX [11]
ERROR: Failed to decode file: ../test/issues/gh492/decode_preR13_entities_Assertion 0x800

READ ERROR 0x800
```

  **rurban** added the **invalid CVE** label on Jun 24

ajakk commented on Jul 2

That doesn't necessarily mean the CVE is invalid, just that the description is wrong. That said, did anyone tell MITRE?

Assignees

 **rurban**

Labels

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

