New issue

Jump to bottom

heap-buffer-overflow exists in the function decode_preR13_section_hdr in decode_r11.c #524

Closed **iorra-cifer** opened this issue 20 days ago · 1 comment

Assignees

Labels blocking bug **fuzzing**

Milestone **0.13**

iorra-cifer commented 20 days ago

System info
Ubuntu x86_64, clang 10.0
version: 0.12.4.4643, last commit 93c2512

Command line
./dwg2dxf poc

Poc
poc: poc

AddressSanitizer output
==4080011==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x618000000428 at pc 0x000000480860 bp 0x7ffddb1de850 sp 0x7ffddb1de008
WRITE of size 63 at 0x618000000428 thread T0
#0 0x48085f in strncpy /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_interceptors.cpp:483:5
#1 0x1123350 in decode_preR13_section_hdr /home/SVF-tools/example/libredwg-2/src/decode_r11.c:139:3
#2 0x111d7e1 in decode_preR13 /home/SVF-tools/example/libredwg-2/src/decode_r11.c:762:7
#3 0x4fb4b6 in dwg_decode /home/SVF-tools/example/libredwg-2/src/decode.c:211:17
#4 0x4c6dcc in dwg_read_file /home/SVF-tools/example/libredwg-2/src/dwg.c:254:11
#5 0x4c4a40 in main /home/SVF-tools/example/libredwg-2/programs/dwg2dxf.c:258:15
#6 0x7f7873298c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#7 0x41b649 in _start (/home/SVF-tools/example/libredwg-2/fuzz/dwg2dxf.ci+0x41b649)

0x618000000428 is located 24 bytes inside of 442820362-byte region [0x618000000410,0x61801a64eb1a)
==4080011==AddressSanitizer CHECK failed: /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_descriptions.cpp:175 "((id)) != (0)" (0x0, 0x0)
#0 0x49bf3e in __asan::AsanCheckFailed(char const*, int, char const*, unsigned long long, unsigned long long) /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_rtl.cpp:73:5
#1 0x4b045f in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long long, unsigned long long) /home/brian/src/final/llvm-project/compiler-rt/lib/sanitizer_common/sanitizer_termination.cpp:78:5
#2 0x4245db in __asan::HeapAddressDescription::Print() const /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_descriptions.cpp
#3 0x427425 in __asan::ErrorGeneric::Print() /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_errors.cpp:591:20
#4 0x497ba8 in __asan::ScopedInErrorReport::~ScopedInErrorReport() /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_report.cpp:141:50
#5 0x4997dd in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, unsigned int, bool) /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_report.cpp:474:1
#6 0x480881 in strncpy /home/brian/src/final/llvm-project/compiler-rt/lib/asan/asan_interceptors.cpp:483:5
#7 0x1123350 in decode_preR13_section_hdr /home/SVF-tools/example/libredwg-2/src/decode_r11.c:139:3
#8 0x111d7e1 in decode_preR13 /home/SVF-tools/example/libredwg-2/src/decode_r11.c:762:7
#9 0x4fb4b6 in dwg_decode /home/SVF-tools/example/libredwg-2/src/decode.c:211:17
#10 0x4c6dcc in dwg_read_file /home/SVF-tools/example/libredwg-2/src/dwg.c:254:11
#11 0x4c4a40 in main /home/SVF-tools/example/libredwg-2/programs/dwg2dxf.c:258:15
#12 0x7f7873298c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
#13 0x41b649 in _start (/home/SVF-tools/example/libredwg-2/fuzz/dwg2dxf.ci+0x41b649)

rurban self-assigned this 11 days ago

rurban added a commit that referenced this issue 10 days ago

`decode_r11: failing dwg_get_first_object TABLE_CONTROL` ... ✕ 69b4132

rurban added a commit that referenced this issue 10 days ago

`decode_r11: failing dwg_get_first_object TABLE_CONTROL` ... ✓ 0075d17

rurban commented 10 days ago Contributor

Fixed in branch smoke/gh524-fuzz-r11

rurban added bug blocking **fuzzing** labels 10 days ago

rurban added this to the **0.13** milestone 10 days ago

rurban added a commit that referenced this issue 10 days ago

`decode_r11: failing dwg_get_first_object TABLE_CONTROL` ... ✓ 84d938b

rurban closed this as completed 3 days ago

Assignees

rurban

Labels

blocking bug **fuzzing**

Projects

None yet

Milestone

0.13

Development

No branches or pull requests

2 participants