New issue

Jump to bottom

Some heap_overflow bug #190

Closed skyvast404 opened this issue on Jan 16, 2020 · 5 comments

Assignees

Labels bug fuzzing

Milestone 0.11

skyvast404 commented on Jan 16, 2020

Hi, I got some bugs which you can reproduce `dxf2dwg $PoC -o /dev/null` .Thses bugs work on version `0.10.1.2685` and `earlier` .

skyvast404 commented on Jan 16, 2020 • edited Author

Heap over flow1

==9430==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000515c8 at pc 0x7f0679221526 bp 0x7fff931e9240 sp 0x7fff931e9230
READ of size 8 at 0x6020000515c8 thread T0
#0 0x7f0679221525 in add_MLINE /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:4637
#1 0x7f06792532d4 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:5930
#2 0x7f067925fcbd in dxf_blocks_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6955
#3 0x7f067926989a in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7679
#4 0x7f0678382ee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
#5 0x55ef2f125465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
#6 0x7f0677a8db96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#7 0x55ef2f124489 in _start (/home/skyvast/Documents/asan_libredwg/bin/dxf2dwg+0x2489)

0x6020000515c8 is located 8 bytes to the left of 16-byte region [0x6020000515d0,0x6020000515e0)
freed by thread T0 here:
#0 0x7f06798117b8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7b8)
#1 0x7f06791e3788 in dxf_free_pair /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:285
#2 0x7f067925ccd6 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6699
#3 0x7f067925fcbd in dxf_blocks_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6955
#4 0x7f067926989a in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7679
#5 0x7f0678382ee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
#6 0x55ef2f125465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
#7 0x7f0677a8db96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
#0 0x7f0679811d38 in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xded38)
#1 0x7f06791e1465 in xcalloc /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:76
#2 0x7f06791e37b0 in dxf_read_pair /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:292
#3 0x7f067925cce5 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6700
#4 0x7f067925fcbd in dxf_blocks_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6955
#5 0x7f067926989a in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7679
#6 0x7f0678382ee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
#7 0x55ef2f125465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
#8 0x7f0677a8db96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:4637 in add_MLINE
Shadow bytes around the buggy address:
0x0c0480002260: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c0480002270: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c0480002280: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c0480002290: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c04800022a0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa 01 fa
=>0x0c04800022b0: fa fa fd fd fa fa fd fd fa[fa]fd fd fa fa fd fd
0x0c04800022c0: fa fa 00 00 fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800022d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800022e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c04800022f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0480002300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==9430==ABORTING

skyvast404 commented on Jan 16, 2020 Author

Heap_overflow2

==9471==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000204a8 at pc 0x7f66ed6bc79e bp 0x7fff91c13050 sp 0x7fff91c13040
READ of size 8 at 0x6020000204a8 thread T0
#0 0x7f66ed6bc79d in add_MLINE /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:4645
#1 0x7f66ed6ee2d4 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:5930
#2 0x7f66ed6facbd in dxf_blocks_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6955
#3 0x7f66ed70489a in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7679
#4 0x7f66ec81dee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
#5 0x55a8060bf465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
#6 0x7f66ebf28b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#7 0x55a8060be489 in _start (/home/skyvast/Documents/asan_libredwg/bin/dxf2dwg+0x2489)

0x6020000204a8 is located 8 bytes to the left of 16-byte region [0x6020000204b0,0x6020000204c0)
allocated by thread T0 here:
#0 0x7f66edcacd38 in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xded38)
#1 0x7f66ed67c465 in xcalloc /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:76
#2 0x7f66ed67e7b0 in dxf_read_pair /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:292
#3 0x7f66ed6f7ce5 in new_object /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6700
#4 0x7f66ed6facbd in dxf_blocks_read /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:6955
#5 0x7f66ed70489a in dwg_read_dxf /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:7679
#6 0x7f66ec81dee7 in dxf_read_file /home/skyvast/Documents/libredwg-0.10.1.2677/src/dwg.c:319
#7 0x55a8060bf465 in main /home/skyvast/Documents/libredwg-0.10.1.2677/programs/dxf2dwg.c:255
#8 0x7f66ebf28b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/skyvast/Documents/libredwg-0.10.1.2677/src/in_dxf.c:4645 in add_MLINE
Shadow bytes around the buggy address:
0x0c047fffc040: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fffc050: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fffc060: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fffc070: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x0c047fffc080: fa fa fd fd fa fa fd fd fa fa 01 fa fa fa fd fd
=>0x0c047fffc090: fa fa fd fd fa[fa]00 00 fa fa fa fa fa fa fa fa
0x0c047fffc0a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fffc0b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fffc0c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fffc0d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fffc0e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==9471==ABORTING
```

skyvast404 commented on Jan 16, 2020 — Author

PoC here.
heap_overflow.zip

rurban self-assigned this on Jan 16, 2020

rurban added the bug label on Jan 16, 2020

rurban added this to the **0.11** milestone on Jan 16, 2020

rurban commented on Jan 16, 2020 — Contributor

Thanks, I can repro all

rurban added the **fuzzing** label on Jan 16, 2020

rurban added a commit that referenced this issue on Jan 16, 2020

`indxf: more NULL ptr protections` ··· `41ff7af`

rurban closed this as completed on Jan 16, 2020

---

skyvast404 commented on Jul 19, 2020 — Author

These bugs credited by ADLab.
CVE-2020-15807

Assignees
rurban

Labels
bug **fuzzing**

Projects
None yet

Milestone
0.11

Development
No branches or pull requests

2 participants