Xfig Tickets

Xfig is a diagramming tool

Brought to you by: tklxfiguser

#125 DoubleFree-readpics.c-62-free_stream

Milestone: fig2dev **Status:** closed **Owner:** nobody **Labels:** None
Updated: 2021-08-22 **Created:** 2021-07-19 **Creator:** HungChun Chiu **Private:** No

System info

Ubuntu 16.04 xenial, gcc (Ubuntu 5.5.0-12ubuntu1), fig2dev (latest master a4c6e1)

Command line

./fig2dev -L pdf -G .25:1cm -j -m 2 -N -P -x 3 -y 4 @@ /dev/null

Output

```
No such picture file: ../../fig2dev/ 0 0 675 0 675 375 0  0 0 5
*** Error in `../../fig2dev': double free or corruption (!prev): 0x0000000000cfc030 ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x777f5)[0x7f7fd7b6f7f5]
/lib/x86_64-linux-gnu/libc.so.6(+0x8038a)[0x7f7fd7b7838a]
/lib/x86_64-linux-gnu/libc.so.6(cfree+0x4c)[0x7f7fd7b7c58c]
../../fig2dev[0x4bbb2b]
../../fig2dev[0x47accd]
../../fig2dev[0x411b24]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0)[0x7f7fd7b18840]
../../fig2dev[0x402c09]
======= Memory map: ========
00400000-004ec000 r-xp 00000000 08:11 27664590                           ../../fig2dev
006ec000-006ed000 r--p 000ec000 08:11 27664590                           ../../fig2dev
006ed000-00700000 rw-p 000ed000 08:11 27664590                           ../../fig2dev
00700000-0071b000 rw-p 00000000 00:00 0
00cfb000-00d1c000 rw-p 00000000 00:00 0                                  [heap]
7f7fd0000000-7f7fd0021000 rw-p 00000000 00:00 0
7f7fd0021000-7f7fd4000000 ---p 00000000 00:00 0
7f7fd7579000-7f7fd7590000 r-xp 00000000 08:02 12582916                   /lib/x86_64-linux-
7f7fd7590000-7f7fd778f000 ---p 00017000 08:02 12582916                   /lib/x86_64-linux-
7f7fd778f000-7f7fd7790000 r--p 00016000 08:02 12582916                   /lib/x86_64-linux-
7f7fd7790000-7f7fd7791000 rw-p 00017000 08:02 12582916                   /lib/x86_64-linux-
7f7fd7791000-7f7fd7af8000 r--p 00000000 08:02 38010883                   /usr/lib/locale/lo
7f7fd7af8000-7f7fd7cb8000 r-xp 00000000 08:02 12583571                   /lib/x86_64-linux-
7f7fd7cb8000-7f7fd7eb8000 ---p 001c0000 08:02 12583571                   /lib/x86_64-linux-
7f7fd7eb8000-7f7fd7ebc000 r--p 001c0000 08:02 12583571                   /lib/x86_64-linux-
7f7fd7ebc000-7f7fd7ebe000 rw-p 001c4000 08:02 12583571                   /lib/x86_64-linux-
7f7fd7ebe000-7f7fd7ec2000 rw-p 00000000 00:00 0
7f7fd7ec2000-7f7fd7fca000 r-xp 00000000 08:02 12583566                   /lib/x86_64-linux-
7f7fd7fca000-7f7fd81c9000 ---p 00108000 08:02 12583566                   /lib/x86_64-linux-
7f7fd81c9000-7f7fd81ca000 r--p 00107000 08:02 12583566                   /lib/x86_64-linux-
7f7fd81ca000-7f7fd81cb000 rw-p 00108000 08:02 12583566                   /lib/x86_64-linux-
7f7fd81cb000-7f7fd81e4000 r-xp 00000000 08:02 12583082                   /lib/x86_64-linux-
7f7fd81e4000-7f7fd83e3000 ---p 00019000 08:02 12583082                   /lib/x86_64-linux-
7f7fd83e3000-7f7fd83e4000 r--p 00018000 08:02 12583082                   /lib/x86_64-linux-
7f7fd83e4000-7f7fd83e5000 rw-p 00019000 08:02 12583082                   /lib/x86_64-linux-
7f7fd83e5000-7f7fd8409000 r-xp 00000000 08:02 12583492                   /lib/x86_64-linux-
7f7fd8409000-7f7fd8608000 ---p 00024000 08:02 12583492                   /lib/x86_64-linux-
7f7fd8608000-7f7fd8609000 r--p 00023000 08:02 12583492                   /lib/x86_64-linux-
7f7fd8609000-7f7fd860a000 rw-p 00024000 08:02 12583492                   /lib/x86_64-linux-
7f7fd860a000-7f7fd8630000 r-xp 00000000 08:02 12583562                   /lib/x86_64-linux-
7f7fd87fb000-7f7fd8800000 rw-p 00000000 00:00 0
7f7fd882e000-7f7fd882f000 rw-p 00000000 00:00 0
7f7fd882f000-7f7fd8830000 r--p 00025000 08:02 12583562                   /lib/x86_64-linux-
7f7fd8830000-7f7fd8831000 rw-p 00026000 08:02 12583562                   /lib/x86_64-linux-
7f7fd8831000-7f7fd8832000 rw-p 00000000 00:00 0
7ffc8c5c7000-7ffc8c5e8000 rw-p 00000000 00:00 0                          [stack]
7ffc8c5ec000-7ffc8c5ee000 r--p 00000000 00:00 0                          [vvar]
7ffc8c5ee000-7ffc8c5f0000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
[1]    32228 abort      ../../fig2dev -L
```

AddressSanitizer output

```
No such picture file: ../../fig2dev/ 0 0 675 0 675 375 0  0 0 5
=================================================================
==28522==ERROR: AddressSanitizer: attempting double-free on 0x610000007d40 in thread T0:
    #0 0x7f58f241532a in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9832a)
    #1 0x519594 in free_stream ../../fig2dev/fig2dev/dev/readpics.c:62
    #2 0x4b2b32 in genps_line ../../fig2dev/fig2dev/dev/genps.c:1674
    #3 0x412a7d in gendev_objects ../../fig2dev/fig2dev/fig2dev.c:1008
    #4 0x411481 in main ../../fig2dev/fig2dev/fig2dev.c:485
    #5 0x7f58f188b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #6 0x4032f8 in _start (/home/qiuhongjun/AlphaFuzz-Experiment/results/crashes-binary/gcc-

0x610000007d40 is located 0 bytes inside of 180-byte region [0x610000007d40,0x610000007df4)
freed by thread T0 here:
    #0 0x7f58f241532a in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9832a)
    #1 0x519594 in free_stream ../../fig2dev/fig2dev/dev/readpics.c:62
    #2 0x51a022 in open_stream ../../fig2dev/fig2dev/dev/readpics.c:211
    #3 0x4b2aa8 in genps_line ../../fig2dev/fig2dev/dev/genps.c:1672
    #4 0x412a7d in gendev_objects ../../fig2dev/fig2dev/fig2dev.c:1008
    #5 0x411481 in main ../../fig2dev/fig2dev/fig2dev.c:485
    #6 0x7f58f188b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

previously allocated by thread T0 here:
    #0 0x7f58f2415662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
    #1 0x519f58 in open_stream ../../fig2dev/fig2dev/dev/readpics.c:199
    #2 0x4b2aa8 in genps_line ../../fig2dev/fig2dev/dev/genps.c:1672
    #3 0x412a7d in gendev_objects ../../fig2dev/fig2dev/fig2dev.c:1008
    #4 0x411481 in main ../../fig2dev/fig2dev/fig2dev.c:485
    #5 0x7f58f188b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: double-free ??:0 __interceptor_free
==28522==ABORTING
```

1 Attachments

POC_DoubleFree-readpics.c-62-free_stream.zip

Discussion

tkl - *2021-07-19*

- **status**: open --> pending

tkl - *2021-07-19*

Fixed with commit [899ea1].

Related

Commit: [899ea1]

tkl - *2021-08-22*

- **status**: pending --> closed

Log in to post a comment.