Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

#61 Segmentation Fault in read_objects() function

Milestone: xfig **Status:** closed **Owner:** nobody **Labels:** None
Updated: 2020-12-21 **Created:** 2019-12-12 **Creator:** Suhwan Song **Private:** No

Hi,
I found a Segmentation Fault in read_objects() at read.c:459
Please run following command to reproduce it,

```
fig2dev -L box $PoC
```

Here's log

```
ASAN:DEADLYSIGNAL
=================================================================
==31429==ERROR: AddressSanitizer: SEGV on unknown address 0x55b05140a000 (pc 0x55b05100e77a
==31429==The signal is caused by a READ memory access.
    #0 0x55b05100e779 in read_objects fig2dev-3.2.7b/fig2dev/read.c:459
    #1 0x55b05100d1d3 in readfp_fig fig2dev-3.2.7b/fig2dev/read.c:172
    #2 0x55b05100d0a9 in read_fig fig2dev-3.2.7b/fig2dev/read.c:142
    #3 0x55b051004ef3 in main fig2dev-3.2.7b/fig2dev/fig2dev.c:422
    #4 0x7fb59892db96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55b050ff5979 in _start (fig2dev-3.2.7b+0x6e979)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV fig2dev-3.2.7b/fig2dev/read.c:459 in read_objects
==31429==ABORTING
```

fig2dev Version 3.2.7b
I also tested this in git Commit [3065ab] and can reproduce it.

1 Attachments

id:000121,sig:06,src:001023+000177,op:splice,rep:128

Related

Commit: [3065ab]

Discussion

tkl - *2020-01-06*

- **status**: open --> pending
- **xfig / fig2dev**: xfig --> fig2dev

tkl - *2020-01-06*

Fixed with commit [41b9bb].

Related

Commit: [41b9bb]

tkl - *2020-12-21*

- **status**: pending --> closed
- **xfig / fig2dev**: fig2dev --> xfig

Log in to post a comment.

SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support
Site Documentation
Site Status