# Xfig Tickets

**Xfig is a diagramming tool**
**Brought to you by: tklxfiguser**

## #62 Segmentation Fault in gencgm_start() 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 gencgm_start() at gencgm.c:233
Please run following command to reproduce it,

```
fig2dev -L cgm $PoC
```

Here's log

```
ASAN:DEADLYSIGNAL
=================================================================
==29566==ERROR: AddressSanitizer: SEGV on unknown address 0x5571b0e7f00c (pc 0x5571b0a958b2
==29566==The signal is caused by a READ memory access.
    #0 0x5571b0a958b1 in gencgm_start fig2dev-3.2.7b/fig2dev/dev/gencgm.c:233
    #1 0x5571b0a7b946 in gendev_objects fig2dev-3.2.7b/fig2dev/fig2dev.c:995
    #2 0x5571b0a7a2bf in main fig2dev-3.2.7b/fig2dev/fig2dev.c:480
    #3 0x7f9046da9b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #4 0x5571b0a6a979 in _start (fig2dev-3.2.7b+0x6e979)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV fig2dev-3.2.7b/fig2dev/dev/gencgm.c:233 in gencgm_start
==29566==ABORTING
```

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

**1 Attachments**

id:000070,sig:06,src:000124+000241,op:splice,rep:128

**Related**

Commit: [3065ab]

### Discussion

tkl - *2020-01-06*

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

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.

San Diego, CA 92101
+1 (858) 454-5900

## Resources

Support
Site Documentation
Site Status