



Xfig Tickets

Xfig is a diagramming tool
Brought to you by: [tklxfiguser](#)

#75 global-buffer-overflow in put_font at genpict2e.c:2229

Milestone: [fig2dev](#)

Status: closed

Owner: nobody

Labels: None

Updated: 2020-12-21

Created: 2019-12-28

Creator: [Suhwan Song](#)

Private: No

Hi,

I found a global-buffer-overflow in put_font at genpict2e.c:2229

Please run following command to reproduce it,

fig2dev -L pict2e \$PoC

ASAN LOG

```
==36598==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000c4f858 at pc 0x000000c4f858
READ of size 8 at 0x000000c4f858 thread T0
#0 0x7614cf in put_font /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:2229:7
#1 0x7614cf in genpict2e_text /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:2278
#2 0x54b8bb in gendev_objects /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:1003:6
#3 0x54b8bb in main /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:480
#4 0x7fb82753eb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:342
#5 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9)

0x000000c4f858 is located 8 bytes to the left of global variable 'texfonts' defined in 'genpict2e.c'
0x000000c4f858 is located 52 bytes to the right of global variable 'default_color' defined in 'genpict2e.c'
SUMMARY: AddressSanitizer: global-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:2229:7
Shadow bytes around the buggy address:
  0x000000181eb0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00
  0x000000181ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000000181ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000000181ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000000181ef0: 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 f9
=>0x000000181f00: f9 f9 f9 f9 04 f9 f9 f9 f9 f9[f9]00 00 00 00 00
  0x000000181f10: 00 00 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x000000181f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000000181f30: 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9
  0x000000181f40: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 04 f9 f9 f9 f9
  0x000000181f50: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 f9 f9
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
==36598==ABORTING
```

fig2dev Version 3.2.7b

I also tested this in git Commit [\[3065ab\]](#) and can reproduce it.


1 Attachments


[id:000046,sig:06,src:000309,op:havoc,rep:8](#)


Related


[Commit: \[3065ab\]](#)

Discussion


tkl - 2020-01-26

• status: open -> pending

tkl - 2020-01-26



Log in



Fixed with commit [d70e4b]

a comment

20-12-21

Related

Commit: [d70e4b]

status: pending -> closed

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status



© 2022 Slashdot Media. All Rights Reserved.

[Terms](#)

[Privacy](#)

[Opt Out](#)

[Advertise](#)