



Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tlkxfiguser

#78 stack-buffer-overflow in genptk_text at genptk.c:618



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 stack-buffer-overflow in genptk_text at genptk.c:618

fig2dev Version 3.2.7b
commit 93795dd396730c80e63767dede777f4cb7dc383

Please run following command to reproduce it,

```
fig2dev -L ptk $PoC
```

ASAN LOG

```
==45827==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fff76457e80 at pc 0x0000000000000000
WRITE of size 1 at 0x7fff76457e80 thread T0
#0 0x841290 in genptk_text /home/tmp/mcj-fig2dev/fig2dev/dev/genptk.c:618:13
#1 0x54ba7b in gendev_objects /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:1012:6
#2 0x54ba7b in main /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:489
#3 0x7f8360406b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:308
#4 0x41b429 in _start (/home/tmp/fig2dev+0x41b429)

Address 0x7fff76457e80 is located in stack of thread T0 at offset 2080 in frame
#0 0x83e5ef in genptk_text /home/tmp/mcj-fig2dev/fig2dev/dev/genptk.c:520

This frame has 1 object(s):
  [32, 2080) 'stfp' (line 521) <== Memory access at offset 2080 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genptk.c:618
Shadow bytes around the buggy address:
  0x10006ec82f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec82f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec82fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec82fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec82fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10006ec82fd0:[f3]f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3 f3
  0x10006ec82fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec82ff0: 00 00 00 00 f1 f1 f1 f1 00 00 00 00 00 00 00 00
  0x10006ec83000: 00 00 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x10006ec83010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006ec83020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==45827==ABORTING
```

1 Attachments

[id:000085,sig:06,src:000765+000189,op:splice,rep:16](#)


Discussion



tlk - 2020-01-06

%

• status: open -> pending

[Log in](#) 

2020-01-06

2012-12-21

•Fixed with commit [\[41b9bb\]](#).

Related

[Commit: \[41b9bb\]](#)

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

