



## Xfig Tickets

Xfig is a diagramming tool

Brought to you by: tlkxfiguser

### #76 stack-buffer-overflow in genpstrx\_text at genpstricks.c:2732



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 genpstrx\_text at genpstricks.c:2732  
Please run following command to reproduce it,

```
fig2dev -L pstricks $PoC
```

#### ASAN LOG

```
==48149==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffcd1c7b00 at pc 0x0000000000000000
WRITE of size 35 at 0x7ffcd1c7b00 thread T0
#0 0x448239 in vsprintf (/home/tmp/fig2dev+0x448239)
#1 0x448566 in __interceptor_sprintf (/home/tmp/fig2dev+0x448566)
#2 0x81943b in genpstrx_text /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:2732:5
#3 0x54b8bb in gendev_objects /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:1003:6
#4 0x54b8bb in main /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:480
#5 0x7fb45a113b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:342
#6 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9)

Address 0x7ffcd1c7b00 is located in stack of thread T0 at offset 65856 in frame
#0 0x817a5f in genpstrx_text /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:2714

This frame has 2 object(s):
[32, 65568) 'formatted_text' (line 2716)
[65824, 65856) 'angle' (line 2717) <== Memory access at offset 65856 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/fig2dev+0x448239) in vsprintf
Shadow bytes around the buggy address:
 0x100079a30f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30f30: 00 00 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2
 0x100079a30f40: f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2
 0x100079a30f50: f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 f2 00 00 00 00
=>0x100079a30f60:[f3]f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30f70: f1 f1 f1 f1 00 00 00 00 00 00 00 00 00 00 f3 f3
 0x100079a30f80: f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x100079a30fb0: 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
==48149==ABORTING
```

fig2dev Version 3.2.7b

#### 1 Attachments


[id:000014,sig:06,src:000006+000127,op:splice,rep:2](#)

#### Discussion




Dr. Werner Fink - 2020-01-28

The attached patch add some sanity checks about correct radians used for angles ... this avoids the overflow in `sprintf` on `angle` character array in `genpstrx_text()` of

[Log in](#)


[fio?dev/dav/gangetricks.c](#)  
 a comment  
 by [Werner Fink](#) · 2020-01-29





Status: pending pending

Commented on this issue, which was open at the time I wrote/rejected it and the 2 days between them.

Last edit: Dr. Werner Fink · 2020-01-28

☐ Issue 76, patch were paired as a pair, possibly probably by say a Tabby input fuzzers, and those are happy with an exit.





Related

[Dr. Werner Fink - 2020-01-28](#)

[Commit: \[acccc8\]](#)

I'm fine with as you're the expert here, I've only debugged it a bit :)

## 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

