



Xfig Tickets

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

#77 global-buffer-overflow in shade_or_tint_name_after_declare_color at genpstricks.c:1135



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 shade_or_tint_name_after_declare_color at genpstricks.c:1135
Please run following command to reproduce it,

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

ASAN LOG

```
Invalid color number -1674115757 at line 37, using default color.  
An open polygon at line 38 - close it.  
=====22079==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000c5a81c at pc 0x0000000000000000  
READ of size 4 at 0x000000c5a81c thread T0  
#0 0x80aeb4 in shade_or_tint_name_after_declare_color /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:1135  
#1 0x80aeb4 in format_options /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:1859  
#2 0x7fa81d in genpstrx_line /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:2270:7  
#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 0x7ff8beedb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:308  
#6 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9)  
  
0x000000c5a81c is located 4 bytes to the left of global variable 'color_table' defined in 'dev/genpstricks.c:1135'  
0x000000c5a81c is located 44 bytes to the right of global variable 'dev_pstricks' defined in 'dev/genpstricks.c:1135'  
SUMMARY: AddressSanitizer: global-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:1135  
Shadow bytes around the buggy address:  
 0x000000801834b0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9  
 0x000000801834c0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9  
 0x000000801834d0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9  
 0x000000801834e0: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 00 f9 f9 f9 f9  
 0x000000801834f0: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 f9 f9  
=>0x00000080183500: f9 f9 f9[f9]00 00 00 00 00 00 00 00 00 00 00 00 00  
 0x00000080183510: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 0x00000080183520: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 0x00000080183530: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 0x00000080183540: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 0x00000080183550: 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  
==22079==ABORTING
```

fig2dev Version 3.2.7b

1 Attachments

[id:000128,sig:06,src:000147,op:havoc,rep:2](#)

Discussion




Dr. Werner Fink - 2020-01-27



Seems that the default color handling from `dev/gentikz.c` is simply missed in `dev/genpstricks.c` hence the offset in `color_table` interferes with `dev_pstricks`

Log in



a commit
s77,028

2020-02-05

Status: pending pending

The issue here is, that an area is filled with the tinted default color. For line colors and solid fills, pstricks knows to handle the default color, i.e., not issuing any color setting command. The result is, that the color from the environment remains. However, pstricks does not know how to tint or shade an unknown color, hence there the default color is taken as black. The error was, that the tinted default color was not handled correctly. Commit [\[639c36\]](#) fixes this issue.

Related

[Commit: \[639c36\]](#)

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

