Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

#72 global-buffer-overflow in set_fill at genge.c:446

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 set_fill at genge.c:446
Please run following command to reproduce it,

```
fig2dev -L ge $PoC
```

ASAN LOG

```
Invalid color number -16 at line 33, using default color.
=================================================================
==3081==ERROR: AddressSanitizer: global-buffer-overflow on address 0x0000009b325c at pc 0x0
READ of size 4 at 0x0000009b325c thread T0
    #0 0x6953ef in set_fill /home/tmp/mcj-fig2dev/fig2dev/dev/genge.c:446:27
    #1 0x6953ef in genge_line /home/tmp/mcj-fig2dev/fig2dev/dev/genge.c:143
    #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 0x7fbb4e7bcb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-s
    #5 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9)

0x0000009b325c is located 4 bytes to the left of global variable 'GE_COLORS' defined in 'ge
0x0000009b325c is located 53 bytes to the right of global variable '<string literal>' defin
  '<string literal>' is ascii string 'c%02d '
SUMMARY: AddressSanitizer: global-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genge.c
Shadow bytes around the buggy address:
  0x00008012e5f0: f9 f9 f9 f9 00 00 02 f9 f9 f9 f9 f9 00 00 f9 f9
  0x00008012e600: f9 f9 f9 f9 00 07 f9 f9 f9 f9 f9 f9 00 00 00 03
  0x00008012e610: f9 f9 f9 f9 00 00 00 00 00 00 02 f9 f9 f9 f9 f9
  0x00008012e620: 00 00 00 00 00 00 00 04 f9 f9 f9 f9 00 06 f9 f9
  0x00008012e630: f9 f9 f9 f9 00 03 f9 f9 f9 f9 f9 f9 00 03 f9 f9
=>0x00008012e640: f9 f9 f9 f9 07 f9 f9 f9 f9 f9[f9]00 00 00 00
  0x00008012e650: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9
  0x00008012e660: 07 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9
  0x00008012e670: 05 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9
  0x00008012e680: 07 f9 f9 f9 f9 f9 f9 f9 00 04 f9 f9 f9 f9 f9 f9
  0x00008012e690: 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
==3081==ABORTING
```

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

1 Attachments

id:000017,sig:06,src:000048,op:havoc,rep:2

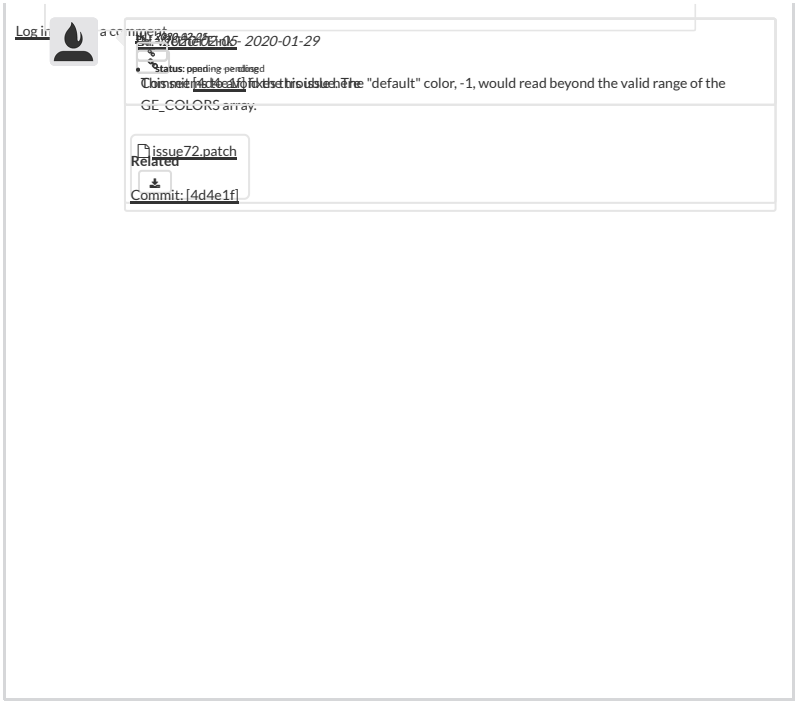
Related

Commit: [3065ab]

Discussion

Dr. Werner Fink - *2020-01-27*

Looks similar to missing default color of issue #77



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