



Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

#73 global-buffer-overflow in set color at genge.c:437 3 Milestone: fig2dev Status: closed Owner: nobody Labels: None Updated: 2020-12-21 Created: 2019-12-28 Creator: Suhwan Song Private: No I found a global-buffer-overflow in set color at genge.c:437 Please run following command to reproduce it, fig2dev -L ge \$PoC ASAN LOG Cannot locate user color 41, using default color at line 10. ==1767==ERROR: AddressSanitizer: global-buffer-overflow on address 0x0000009b325c at pc 0x0 READ of size 4 at 0x0000009b325c thread T0 #0 0x69b1f7 in set color /home/tmp/mcj-fig2dev/fig2dev/dev/genge.c:437:23 #1 0x69b1f7 in genge_arc /home/tmp/mcj-fig2dev/fig2dev/dev/genge.c:345 #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 0x7f219e288b96 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>' define '<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 00 00 f9 f9 0x00008012e600: f9 f9 f9 f9 00 07 f9 f9 f9 f9 f9 o0 00 00 03 0x00008012e610: f9 f9 f9 f9 00 00 00 00 00 02 f9 f9 f9 f9 0x00008012e620: 00 00 00 00 00 00 04 f9 f9 f9 f0 00 06 f9 f9 0x00008012e630: f9 f9 f9 f9 00 03 f9 f9 f9 f9 f9 00 03 f9 f9 =>0x00008012e640: f9 f9 f9 f9 07 f9 f9 f9 f9 f9 f9[f9]00 00 00 0x00008012e650: 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 0x00008012e680: 07 f9 f9 f9 f9 f9 f9 00 04 f9 f9 f9 f9 f9 Shadow byte legend (one shadow byte represents 8 application bytes): Addressable: Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa Freed heap region: Stack left redzone: Stack mid redzone: f2 Stack right redzone: f3 Stack after return: Stack use after scope: f8 Global redzone: f9 Global init order: Poisoned by user: £7 Container overflow: fc Arrav cookie: ac Intra object redzone: ASan internal: fe Left alloca redzone: Right alloca redzone: ==1767==ABORTING fig2dev Version 3.2.7b I also tested this in git Commit [3065ab] and can reproduce it.

1 Attachments

id:000024,sig:06,src:000096+000201,op:splice,rep:2

Related

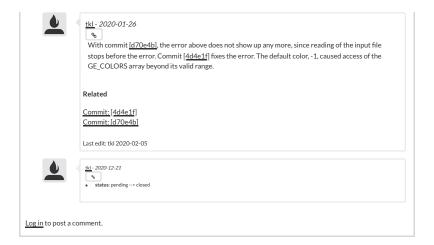
Commit: [3065ab]

Discussion



tkl - 2020 01-26

s status: open --> pending



SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

