



Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

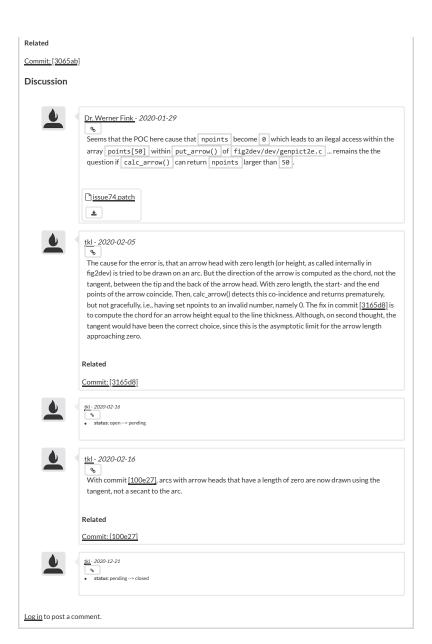
#74 stack-buffer-overflow in put_arrow at genpict2e.c:1191 3 Milestone: fig2dev Status: closed Owner: nobody Labels: None Updated: 2020-12-21 Created: 2019-12-28 Creator: Suhwan Song Private: No I found a stack-buffer-overflow in put arrow at genpict2e.c:1191 Please run following command to reproduce it, fig2dev -L pict2e \$PoC ASAN LOG ==39178==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fffc3316ec8 at pc 0x0 READ of size 4 at 0x7fffc3316ec8 thread T0 #0 0x77150c in put arrow /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:1191:39 #1 0x767f69 in genpict2e_arc /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:2575:6 #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 0x7f8b1eb44b96 in libc start main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-s #5 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9) Address 0x7fffc3316ec8 is located in stack of thread TO at offset 72 in frame #0 0x76d4cf in put_arrow /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2e.c:1152 This frame has 9 object(s): [48, 52) 'sy' (line 1153) [64, 68) 'lx' (line 1153) <== Memory access at offset 72 overflows this variable [80, 480) 'points' (line 1154) <== Memory access at offset 72 underflows this variable [544, 944) 'fillpoints' (line 1154) [1008, 1408) 'clippts' (line 1154) [1472, 1476) 'npoints' (line 1155) [1488, 1492) 'nfillpoints' (line 1155) [1504, 1508) 'nclippts' (line 1155) HINT: this may be a false positive \mathbf{if} your program uses some custom stack unwind mechanism (longjmp and C++ exceptions *are* supported) SUMMARY: AddressSanitizer: stack-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genpict2 Shadow bytes around the buggy address: =>0x10007865add0: f1 f1 f1 f1 04 f2 04 f2 04[f2]00 00 00 00 00 00 0x10007865ae00: 00 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2 0x10007865ae10: f2 f2 f2 f2 00 00 00 00 00 00 00 00 00 00 00 Shadow byte legend (one shadow byte represents 8 application bytes): Addressable: 0.0 Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa Freed heap region: fd Stack left redzone: Stack mid redzone: f2 Stack right redzone: £3 Stack after return: f5 Stack use after scope: Global redzone: Global init order: Poisoned by user: £7 Container overflow: fc Arrav cookie: ac Intra object redzone: bb ASan internal: fe Left alloca redzone: Right alloca redzone: ==39178==ABORTING

fig2dev Version 3.2.7b

I also tested this in git Commit $\underline{[3065ab]}$ and can reproduce it.

1 Attachments

id:000007,sig:06,src:000000,op:havoc,rep:2



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



Privacy