



Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

#76 stack-buffer-overflow in genpstrx text at genpstricks.c:2732 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 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 0x7fffcd1c7b00 at pc 0x0 WRITE of size 35 at 0x7fffcd1c7b00 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-s #6 0x41b3a9 in start (/home/tmp/fig2dev+0x41b3a9) Address 0x7fffcd1c7b00 is located in stack of thread TO at offset 65856 in frame #0 0x817a5f in genpstrx_text /home/tmp/mcj-fig2dev/fig2dev/dev/genpstricks.c:2714 [32, 65568) 'formatted_text' (line 2716) [65824, 65856) 'angle' (line 2717) <== Memory access at offset 65856 overflows this var ${\tt HINT:}\ \ {\tt this}\ \ {\tt may}\ \ {\tt be}\ \ {\tt a}\ \ {\tt false}\ \ {\tt positive}\ \ {\tt if}\ \ {\tt your}\ \ {\tt program}\ \ {\tt uses}\ \ {\tt some}\ \ {\tt custom}\ \ {\tt stack}\ \ {\tt unwind}\ \ {\tt mechanism}$ (longjmp and C++ exceptions *are* supported) SUMMARY: AddressSanitizer: stack-buffer-overflow (/home/tmp/fig2dev+0x448239) in vsprintf Shadow bytes around the buggy address: 0x100079a30f30: 00 00 00 00 00 00 00 00 00 00 00 f2 f2 f2 f2 0x100079a30f50: f2 00 00 00 =>0x100079a30f60:[f3]f3 f3 f3 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 f3 f3 0x100079a30f80: f3 f3 f3 f3 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: £5 Stack use after scope: f8 Global redzone: £9 Global init order: Poisoned by user: £7 Container overflow: fc Arrav cookie: ac Intra object redzone: hh ASan internal: fe Left alloca redzone: Right alloca redzone: ==48149==ABORTING

fig2dev Version 3.2.7b

1 Attachments

id:000014,sig:06,src:000006+000127,op:splice,rep:2

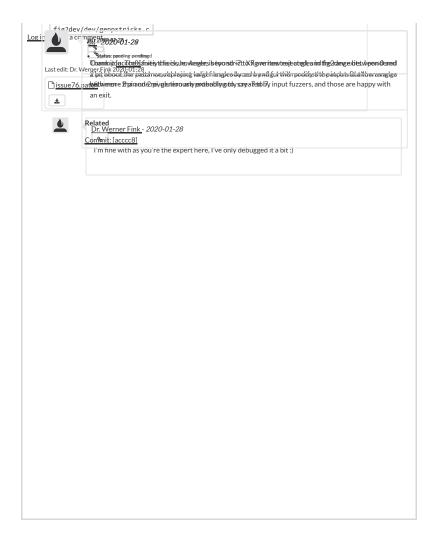
Discussion



Dr. Werner Fink - 2020-01-28

ಹಿ

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



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

