



Xfig Tickets

Xfig is a diagramming tool Brought to you by: tklxfiguser

#63 global-buffer-overflow in conv_pattern_index() function 3 Milestone: xfig Status: closed Owner: nobody Labels: None Updated: 2020-12-21 Created: 2019-12-12 Creator: Suhwan Song Private: No I found a global-buffer-overflow in conv_pattern_index() at gencgm.c:533 $\,$ Please run following command to reproduce it, fig2dev -L cgm \$PoC Here's log An open polygon at line 31 - close it. ==27666==ERROR: AddressSanitizer: global-buffer-overflow on address 0x55d8bbafa358 at pc 0x READ of size 4 at 0x55d8bbafa358 thread T0 #0 0x55d8bb7759d9 in conv pattern index fig2dev-3.2.7b/fig2dev/dev/gencgm.c:533 #1 0x55d8bb775a20 in hatchindex fig2dev-3.2.7b/fig2dev/dev/gencgm.c:543 #2 0x55d8bb776d1d in shape fig2dev=3.2.7b/fig2dev/dev/gencgm.c:638 #3 0x55d8bb77cbc4 in gencgm_line fig2dev-3.2.7b/fig2dev/dev/gencgm.c:1044 #4 0x55d8bb75aa3f in gendev objects fig2dev-3.2.7b/fig2dev/fig2dev.c:1003 #5 0x55d8bb7592bf in main fig2dev-3.2.7b/fig2dev/fig2dev.c:480 #6 0x7fe59b3a7b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #7 0x55d8bb749979 in _start (fig2dev-3.2.7b+0x6e979) ${\tt 0x55d8bbafa358} \text{ is located 0 bytes to the right of global variable 'map_pattern' defined in}$ 0x55d8bbafa358 is located 40 bytes to the left of global variable 'oldfillcolor' defined in SUMMARY: AddressSanitizer: global-buffer-overflow fig2dev-3.2.7b/fig2dev/dev/gencgm.c:533 i Shadow bytes around the buggy address: 0x0abb97757450: 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 =>0x0abb97757460: 00 00 00 00 00 00 00 00 00 00 00[f9]f9 f9 f9 0x0abb977574a0: 04 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 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: Freed heap region: Stack left redzone: f1 Stack mid redzone: Stack right redzone: £3 Stack after return: Stack use after scope: f8 Global redzone: Global init order: f6 Poisoned by user: Container overflow: fc Array cookie: Intra object redzone: bb ASan internal: Left alloca redzone: ca Right alloca redzone: ==27666==ABORTING fig2dev Version 3.2.7b

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

1 Attachments

id:000080,sig:06,src:000791,op:havoc,rep:2

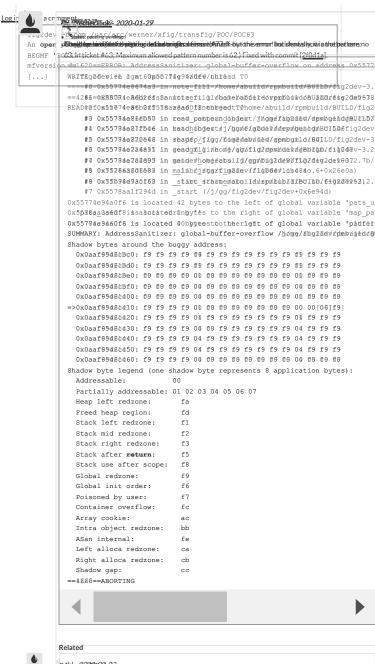
Related

Commit: [3065ab]

Discussion



Dr. Werner Fink - 2020-01-22

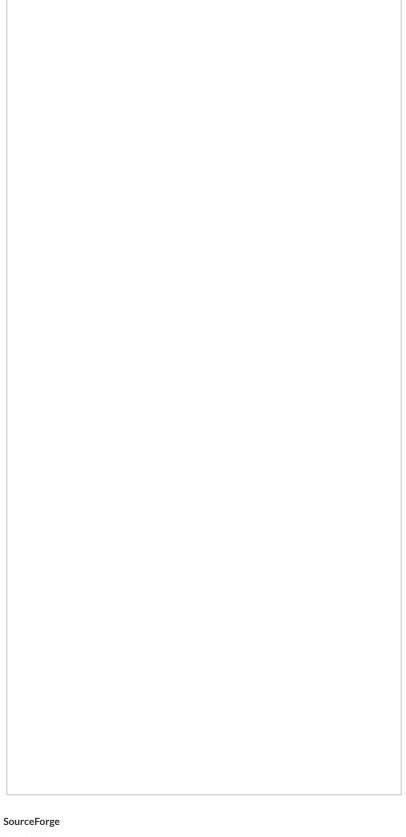


Caklmit929800-93

Las Come (vingo out fig 2 glev 3.2.7b and applying [2f8d1a], i.e., replacing on line 64 of fig2dev/object.h ">" by ">=", here this erro 63poc.fig and the original issue. ">=", here this error does not show up any more. Therefore I believe commit [2f8d1a] fixes this

*

Commit: [2f8d1a]



Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

SourceForge Headquarters

225 Broadway Suite 1600

+1 (858) 454-5900

Resources

Support Site Documentation Site Status



© 2022 Slashdot Media. All Rights Reserved.

Terms Privacy Opt Out Advertise