



Xfig Tickets

Xfig is a diagramming tool Brought to you by: tklxfiguser

#58 global-buffer-overflow in get line() 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 global-buffer-overflow in get line at read.c:1528 Please run following command to reproduce it, fig2dev -L box \$PoC Here's log ==23137==ERROR: AddressSanitizer: global-buffer-overflow on address 0x556239047e7f at pc 0x READ of size 1 at 0x556239047e7f thread T0 #1 0x556238c5e9fb in read objects fig2dev-3.2.7b/fig2dev/read.c:278 #2 0x556238c5e1d3 in readfp_fig fig2dev-3.2.7b/fig2dev/read.c:172 #3 0x556238c5e0a9 in read_fig fig2dev-3.2.7b/fig2dev/read.c:142 #4 0x556238c55ef3 in main fig2dev-3.2.7b/fig2dev/fig2dev.c:422 #6 0x556238c46979 in _start (fig2dev-3.2.7b+0x6e979) 0x556239047e7f is located 59 bytes to the right of global variable 'gif_colnum' defined in 0x556239047e7f is located 1 bytes to the left of global variable 'buf' defined in 'read.c:8 Shadow bytes around the buggy address: 0x0aacc7200fb0: 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 =>0x0aacc7200fc0: 00 00 00 00 00 00 00 04 f9 f9 f9 f9 f9 f9[f9] Shadow byte legend (one shadow byte represents 8 application bytes): Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa Freed heap region: Stack left redzone: Stack mid redzone: Stack right redzone: Stack after return: Stack use after scope: Global redzone: f9 Global init order: Poisoned by user: £7 Container overflow: fc Array cookie: ac Intra object redzone: hh ASan internal: fe Left alloca redzone: Right alloca redzone: ==23137==ABORTING fig2dev Version 3.2.7b

I also tested this in git master and can reproduce it.

1 Attachments

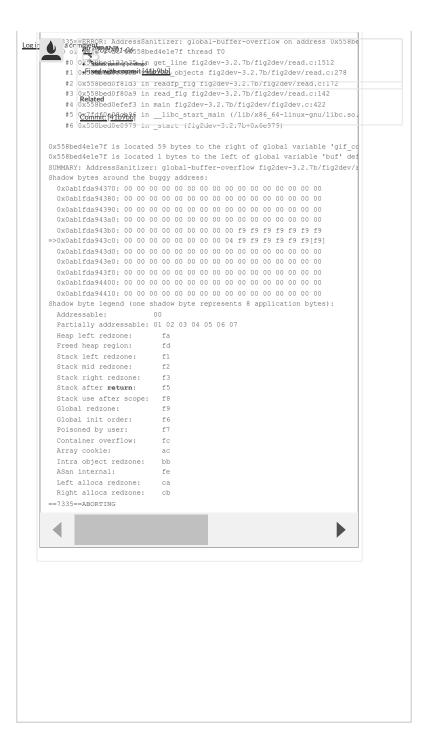
id:000000,sig:06,src:000000,op:havoc,rep:128

Discussion



Suhwan Song - 2019-12-12

Log is incomplete, it's my mistake



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