Xfig Tickets

Xfig is a diagramming tool
Brought to you by: tklxfiguser

#116 [Security] global-buffer-overflow of fig2dev/read.c in function read_objects

Milestone: fig2dev **Status:** closed **Owner:** nobody **Labels:** security (8)
Updated: 2021-08-22 **Created:** 2021-04-19 **Creator:** shanzhuli **Private:** No

Hello Xfig Team
I found an crash error.

System info :
Ubuntu 20.04 : clang 10.0.0 , gcc 9.3.0

fig2dev Version 3.2.8a

Verification steps :
1.Get the source code of fig2dev
2.Compile the fig2dev

```
$ cd fig2dev-3.2.8a
$ ./configure CC="clang -O2 -fno-omit-frame-pointer -g -fsanitize=address" CXX="clang++ -O2
$ make
```

3.run fig2dev
`$ ./fig2dev -L box fig2dev_box_crash`

asan info

```
Invalid color definition at line 11:    0#U75 0 6750 #1 -1 4 -1 -1 0.000 0  0 1 0  -1 0 0,5
Invalid color definition at line 12:     0 i, setting to black (#00000).
=================================================================
==2147685==ERROR: AddressSanitizer: global-buffer-overflow on address 0x5583735f1b08 at pc
WRITE of size 14 at 0x5583735f1b08 thread T0
    #0 0x7f195e0bc714 in vsprintf (/lib/x86_64-linux-gnu/libasan.so.5+0x9e714)
    #1 0x7f195e0bcbce in sprintf (/lib/x86_64-linux-gnu/libasan.so.5+0x9ebce)
    #2 0x558373381445 in read_objects /home/hh/target/fuzzer/xfig/fig2dev-3.2.8a/fig2dev/re
    #3 0x558373381445 in readfp_fig /home/hh/target/fuzzer/xfig/fig2dev-3.2.8a/fig2dev/read
    #4 0x5583733824c3 in read_fig /home/hh/target/fuzzer/xfig/fig2dev-3.2.8a/fig2dev/read.c
    #5 0x55837334b320 in main /home/hh/target/fuzzer/xfig/fig2dev-3.2.8a/fig2dev/fig2dev.c:
    #6 0x7f195dce80b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #7 0x55837334d26d in _start (/home/hh/target/fuzzer/xfig/fig2dev-3.2.8a/fig2dev/fig2dev

0x5583735f1b08 is located 56 bytes to the left of global variable 'support_i18n' defined in
  'support_i18n' is ascii string ''
0x5583735f1b08 is located 0 bytes to the right of global variable 'gif_transparent' defined
SUMMARY: AddressSanitizer: global-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x9e7
Shadow bytes around the buggy address:
  0x0ab0ee6b6310: 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6320: 01 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6330: 00 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6340: 04 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6350: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
=>0x0ab0ee6b6360: 00[f9]f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6370: 01 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6380: 01 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b6390: 01 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b63a0: 01 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
  0x0ab0ee6b63b0: 01 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9 f9 f9 f9 f9
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==2147685==ABORTING
```

Thanks

1 Attachments

fig2dev_box_crash

Discussion

tkl - *2021-04-24*

- **status**: open --> pending
- **private**: Yes --> No

tkl - *2021-04-24*

Fixed with commit [6827c0].

Related

Commit: [6827c0]

tkl - *2021-08-22*

- **status**: pending --> closed

Log in to post a comment.

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

Terms Privacy Opt Out Advertise