Xfig Tickets

Xfig is a diagramming tool

Brought to you by: tklxfiguser

#64 global-buffer-overflow in setfigfont() function

Milestone: xfig **Status:** closed **Owner:** nobody **Labels:** None
Updated: 2020-12-21 **Created:** 2019-12-12 **Creator:** Suhwan Song **Private:** No

Hi
I found a global-buffer-overflow in setfigfont() function at genepic.c:1239
Please run following command to reproduce it,

```
fig2dev -L eepic $PoC
```

Here's log

```
=================================================================
==16081==ERROR: AddressSanitizer: global-buffer-overflow on address 0x55aa8f20b5f8 at pc 0x
READ of size 8 at 0x55aa8f20b5f8 thread T0
    #0 0x55aa8ee6a135 in setfigfont fig2dev-3.2.7b/fig2dev/dev/genepic.c:1239
    #1 0x55aa8ee6a9f5 in genepic_text fig2dev-3.2.7b/fig2dev/dev/genepic.c:1312
    #2 0x55aa8ee1ea3f in gendev_objects fig2dev-3.2.7b/fig2dev/fig2dev.c:1003
    #3 0x55aa8ee1d2bf in main fig2dev-3.2.7b/fig2dev/fig2dev.c:480
    #4 0x7f1a35038b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55aa8ee0d979 in _start (fig2dev-3.2.7b+0x6e979)

0x55aa8f20b5f8 is located 40 bytes to the right of global variable 'texfontseries' defined
0x55aa8f20b5f8 is located 8 bytes to the left of global variable 'texfontshape' defined in
SUMMARY: AddressSanitizer: global-buffer-overflow fig2dev-3.2.7b/fig2dev/dev/genepic.c:1239
Shadow bytes around the buggy address:
  0x0ab5d1e39660: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e39670: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e39680: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e39690: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e396a0: 00 04 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 f9 f9
=>0x0ab5d1e396b0: f9 f9 f9 f9 00 00 00 00 00 00 f9 f9 f9 f9 f9[f9]
  0x0ab5d1e396c0: 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 00 00 00 00
  0x0ab5d1e396d0: 00 00 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x0ab5d1e396e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e396f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ab5d1e39700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==16081==ABORTING
```

fig2dev Version 3.2.7b
I also tested this in git Commit [3065ab] and can reproduce it.

1 Attachments

id:000037,sig:06,src:000306,op:havoc,rep:2

Related

Commit: [3065ab]

Discussion

Dr. Werner Fink - *2020-01-29*

Seems that the fix for CVE-2019-19797 with 41b9bb838a3d544539f6e68aa4f87d70ef7d45ce does mask the original error tkl - *2020-01-29*

- **status**: open --> pending

tkl - *2020-01-29*

Commit [421afa] resolves the original error. I also had applied [00cded], but from the code the first commit is certainly the responsible one. What I tried was:

```
git checkout 41b9bb8^ .
autoreconf -i
./configure CFLAGS="-O0 -ggdb -fsanitize=address"
cd fig2dev
make -sj
./fig2dev -L eepic /tmp/poc64.fig >/dev/null
make clean
git cherry-pick -n 00cdeda 421afa1
make -sj
./fig2dev -L eepic /tmp/poc64.fig >/dev/null
```

Related

Commit: [00cded]
Commit: [421afa]

tkl - *2020-12-21*

- **status**: pending --> closed
- **xfig / fig2dev**: fig2dev --> xfig

Log in to post a comment.

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

Terms Privacy Opt Out Advertise