Xfig Tickets

Xfig is a diagramming tool

Brought to you by: tklxfiguser

#63 global-buffer-overflow in conv_pattern_index() 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 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 0x5
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)

0x55d8bbafa358 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 in
Shadow bytes around the buggy address:
  0x0abb97757410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0abb97757420: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0abb97757430: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0abb97757440: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0abb97757450: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9
=>0x0abb97757460: 00 00 00 00 00 00 00 00 00 00 00[f9]f9 f9 f9 f9
  0x0abb97757470: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0abb97757480: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0abb97757490: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0abb977574a0: 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x0abb977574b0: 04 f9 f9 f9 f9 f9 f9 f9 04 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
==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*

Log in to post a comment.

2020-01-29

- Status: pending

```
fig2dev -L cgm /usr/src/werner/xfig/transfig/POC/POC63
An open ...
BEGMF 'POC63';
mfversion 1;
[...]
```

63; in ticket #63; Maximum allowed pattern number is 62.) Fixed with commit [2f8d1a].

```
==1620==ERROR: AddressSanitizer: global-buffer-overflow on address 0x55774
WRITE of size 1 at 0x55774e94a0f6 thread T0
    #0 0x55774e8674a3 in note_fill /home/abuild/rpmbuild/BUILD/fig2dev-3.2
==4266==ERROR: AddressSanitizer: global-buffer-overflow on address 0x5578a
READ of size 1 at 0x5578aa3a60f8 thread T0
    #0 0x5578aa2eb080 in read_patternd /j/gg/fig2dev/fig2dev/read.c:1
    #1 0x5578aa2e2546 in read_objects /j/gg/fig2dev/fig2dev/read.c:5
    #2 0x5578aa2e0546 in read_fig /j/gg/fig2dev/fig2dev/read.c:241
    #3 0x5578aa2e4895 in readfp_fig /j/gg/fig2dev/fig2dev/read.c:1
    #4 0x5578aa2e2895 in main /home/abuild/rpmbuild/BUILD/fig2dev-3.2.7b/f
    #5 0x7f26a3d6e0a in __libc_start_main (/lib64/libc.so.6+0x26e0a)
    #6 0x5578aa1f5f52 in _start (/home/abuild/rpmbuild/BUILD/fig2dev-3.2.7
    #7 0x5578aa1f294d in _start (/j/gg/fig2dev/fig2dev+0x6e94d)
0x55774e94a0f6 is located 42 bytes to the left of global variable 'pats_us
0x5578aa3a60f8 is located 0 bytes to the right of global variable 'map_pat
0x55774e94a0f6 is located 0 bytes to the right of global variable 'pattern
SUMMARY: AddressSanitizer: global-buffer-overflow /j/gg/fig2dev/fig2dev/re
Shadow bytes around the buggy address:
  0x0aaf5542cbc0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0aaf5542cbd0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0aaf5542cbe0: f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x0aaf5542cbf0: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0aaf5542cc00: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
=>0x0aaf5542cc10: f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9 00 00[06]f9]
  0x0aaf5542cc20: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0aaf5542cc30: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0aaf5542cc40: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0aaf5542cc50: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0aaf5542cc60: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 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
==4266==ABORTING
```

Related

Commit: [2f8d1a]

tkl - *2020-02-03*

Last edit: tkl 2020-01-29

63poc.fig

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

Related

Commit: [2f8d1a]

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