



Xfig Tickets

Xfig is a diagramming tool

Brought to you by: [tklxfiguser](#)

#71 global-buffer-overflow in genmp_writefontmacro_latex at genmp.c:1274

Milestone: [fig2dev](#) Status: closed Owner: nobody Labels: None
Updated: 2020-12-21 Created: 2019-12-28 Creator: [Suhwan Song](#) Private: No

Hi,
I found a global-buffer-overflow in genmp_writefontmacro_latex at genmp.c:1274
Please run following command to reproduce it,

```
fig2dev -L mp $PoC
```

Here's log

```
==17197==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000c7ffd8 at pc 0x0000000000000000
READ of size 8 at 0x000000c7ffd8 thread T0
#0 0x70bc34 in genmp_writefontmacro_latex /home/tmp/mcj-fig2dev/fig2dev/dev/genmp.c:1274
#1 0x70bc34 in genmp_text /home/tmp/mcj-fig2dev/fig2dev/dev/genmp.c:1074
#2 0x54b8bb in gendev_objects /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:1003:6
#3 0x54b8bb in main /home/tmp/mcj-fig2dev/fig2dev/fig2dev.c:480
#4 0x7fab84f5db96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:308
#5 0x41b3a9 in _start (/home/tmp/fig2dev+0x41b3a9)

0x000000c7ffd8 is located 8 bytes to the left of global variable 'texfontfamily' defined in /home/tmp/mcj-fig2dev/fig2dev/dev/genmp.c
SUMMARY: AddressSanitizer: global-buffer-overflow /home/tmp/mcj-fig2dev/fig2dev/dev/genmp.c:1274
Shadow bytes around the buggy address:
 0x0000000187fa0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
 0x0000000187fb0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
 0x0000000187fc0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
 0x0000000187fd0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
 0x0000000187fe0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
=>0x0000000187ff0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
0x0000000188000: 00 00 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 f9 f9
0x0000000188010: f9 f9 f9 f9 00 00 00 00 00 00 00 f9 f9 f9 f9 f9
0x0000000188020: 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9 00 00 00
0x0000000188030: 00 04 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
0x0000000188040: f9 f9 f9 f9 f9 f9 f9 f9 f9 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
==17197==ABORTING
```

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

1 Attachments

[id:000069.sig;06.src:000641.op:havoc.rep:16](#)

Related

[Commit: \[3065ab\]](#)

Discussion




tkl - 2020-01-26
• status: open--> pending



tkl - 2020-01-26

Log in



with commit [d70e4b].
a comment
20-12-21

Related

- status: pending -> closed

[Commit: \[d70e4b\]](#)

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

