New issue

Jump to bottom

Heap-based buffer overflow in the Type2NotDefSplines() function #4085

Closed **fcambus** opened this issue on Jan 3, 2020 · 5 comments

Labels �unțrușted inpüt�

fcambus commented on Jan 3, 2020

Hi,

While fuzzing FontForge with AFL, I found a heap-based buffer overflow in the Type2NotDefSplines() function, in splinesave.c.

Attaching a reproducer (gzipped so GitHub accepts it): test02.sfd.gz

Issue can be reproduced in FontForge 20190801 and with latest Git master by running:

```
fontforge -lang ff -c 'Open("test02.sfd"); Generate("test02.otf")'
```

```
=================================================================
==8320==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000013e8 at pc 0x7fe41192f7bf bp 0x7ffcc7907050 sp 0x7ffcc7907040
WRITE of size 8 at 0x6020000013e8 thread T0
    #0 0x7fe41192f7be in Type2NotDefSplines /home/fcambus/fontforge-20190801/fontforge/splinesave.c:3099
    #1 0x7fe41193030c in SplineFont2ChrsSubrs2 /home/fcambus/fontforge-20190801/fontforge/splinesave.c:3235
    #2 0x7fe411ae5df3 in dumptype2glyphs /home/fcambus/fontforge-20190801/fontforge/tottf.c:2639
    #3 0x7fe411b0f07c in initTables /home/fcambus/fontforge-20190801/fontforge/tottf.c:5750
    #4 0x7fe411b13475 in _WriteTTFFont /home/fcambus/fontforge-20190801/fontforge/tottf.c:6143
    #5 0x7fe411b13611 in WriteTTFFont /home/fcambus/fontforge-20190801/fontforge/tottf.c:6171
    #6 0x7fe4116c60b4 in _DoSave /home/fcambus/fontforge-20190801/fontforge/savefont.c:845
    #7 0x7fe4116c8f7b in GenerateScript /home/fcambus/fontforge-20190801/fontforge/savefont.c:1269
    #8 0x7fe4116df9c4 in bGenerate /home/fcambus/fontforge-20190801/fontforge/scripting.c:2061
    #9 0x7fe41173d6bb in docall /home/fcambus/fontforge-20190801/fontforge/scripting.c:9632
    #10 0x7fe41173e55e in handlename /home/fcambus/fontforge-20190801/fontforge/scripting.c:9745
    #11 0x7fe4117428d0 in term /home/fcambus/fontforge-20190801/fontforge/scripting.c:9983
    #12 0x7fe4117441de in mul /home/fcambus/fontforge-20190801/fontforge/scripting.c:10128
    #13 0x7fe411744ade in add /home/fcambus/fontforge-20190801/fontforge/scripting.c:10174
    #14 0x7fe4117459e7 in comp /home/fcambus/fontforge-20190801/fontforge/scripting.c:10249
    #15 0x7fe41174644d in _and /home/fcambus/fontforge-20190801/fontforge/scripting.c:10293
    #16 0x7fe411746a79 in _or /home/fcambus/fontforge-20190801/fontforge/scripting.c:10325
    #17 0x7fe411747167 in assign /home/fcambus/fontforge-20190801/fontforge/scripting.c:10358
    #18 0x7fe41174884f in expr /home/fcambus/fontforge-20190801/fontforge/scripting.c:10436
    #19 0x7fe41174a4de in ff_statement /home/fcambus/fontforge-20190801/fontforge/scripting.c:10649
    #20 0x7fe41174bb92 in ProcessNativeScript /home/fcambus/fontforge-20190801/fontforge/scripting.c:10796
    #21 0x7fe41174c59f in _CheckIsScript /home/fcambus/fontforge-20190801/fontforge/scripting.c:10894
    #22 0x7fe41174c881 in CheckIsScript /home/fcambus/fontforge-20190801/fontforge/scripting.c:10927
    #23 0x7fe413289be7 in fontforge_main /home/fcambus/fontforge-20190801/fontforgeexe/startui.c:1099
    #24 0x55d5019f01ec in main /home/fcambus/fontforge-20190801/fontforgeexe/main.c:33
    #25 0x7fe4129171e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)
    #26 0x55d5019f010d in _start (/home/fcambus/fontforge-20190801/fontforgeexe/.libs/fontforge+0x110d)

Address 0x6020000013e8 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fcambus/fontforge-20190801/fontforge/splinesave.c:3099 in Type2NotDefSplines
Shadow bytes around the buggy address:
  0x0c047fff8220: fa fa 05 fa fa fa 00 02 fa fa fd fa fa fa 00 00
  0x0c047fff8230: fa fa 00 01 fa fa 07 fa fa fa 01 fa fa fa 01 fa
  0x0c047fff8240: fa fa 01 fa fa fa 00 03 fa fa 00 03 fa fa 00 03
  0x0c047fff8250: fa fa 00 04 fa fa 04 fa fa fa 01 fa fa fa fa fa
  0x0c047fff8260: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c047fff8270: fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa fa
  0x0c047fff8280: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff82a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff82b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==8320==ABORTING
```

fcambus commented on Jan 3, 2020 Author

This issue has been assigned CVE-2020-5496.

NicoleG25 mentioned this issue on Jan 5, 2020

Use-after-free (heap) in the SFD_GetFontMetaData() function #4084

Closed

ctrlcctrlv added the **�unțrușted inpüt�** label on Jan 5, 2020

skef commented on Jan 6, 2020 Contributor

@fcambus This one isn't reproducing for me with either a debug or release build. I'm one unrelated change ahead of the current master `15af0cf`. Can you check again and supply more info about your configuration if you can still reproduce?

fcambus commented on Jan 7, 2020 Author

@skef I can confirm that I can reproduce with `15af0cf`, but that it is fixed with commit `048a91e`.

skef commented on Jan 7, 2020 Contributor

Weird -- that implies the problem was downstream of #4084, which was the only one I fixed first. The relations between these fuzzing symptoms can be counter-intuitive.

I guess we can close this.

ctrlcctrlv commented on Jan 7, 2020 Member

Don't mind if I do 😛

ctrlcctrlv closed this as completed on Jan 7, 2020

erictapen added a commit to erictapen/nixpkgs that referenced this issue on May 25, 2020

`fontforge: patch for CVE-2020-5395 and CVE-2020-5496` ··· `156fc5f`

Assignees

No one assigned

Labels

�unțrușted inpüt�

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants