Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059936/id192_heap_buffer_overflow_sample_otfccdump%2B0x65fc97.zip

Command to reproduce

```
./otfccbuild --pretty [sample file] -o /dev/null
```

Product name & version

```
last github commit code : 617837b
```

Problem Type

```
heap-buffer-overflow
```

Crash Detail

```
==107517==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b000000660 at pc 0x00000065fc98 bp 0x7ffe7eb24290 sp 0x7ffe7eb24288
READ of size 1 at 0x61b000000660 thread T0
    #0 0x65fc97  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
    #1 0x4fe89d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x61b000000660 is located 0 bytes to the right of 1504-byte region [0x61b000000080,0x61b000000660)
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4aecd8)
    #1 0x4fa78f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fa78f)
    #2 0x4f9a31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f9a31)
    #3 0x4f55dc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f55dc)
    #4 0x7fe052acac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
Shadow bytes around the buggy address:
  0x0c367fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff80b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c367fff80c0: 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c367fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8110: 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
==107517==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65fc97)
```