<> Code   ⊙ Issues 1   ⫝ Pull requests   ▶ Actions   ⊞ Projects   ⊘ Security   •••

ᛘ main ▾

Poc / otfcc / **CVE-2022-35056.md**

Cvjark Create CVE-2022-35056.md                    🕘 History

👥 **1 contributor**

≡   74 lines (64 sloc)  │  3.04 KB                              •••

## Product Link

https://github.com/caryll/otfcc

## POC file

https://github.com/Cvjark/Poc/files/9059916/id102_heap_buffer_overflow_sample_otfccdump%2B0x6b0478.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

```
==101583==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6100000000f3
at pc 0x0000006b0479 bp 0x7ffcfed95d00 sp 0x7ffcfed95cf8
READ of size 1 at 0x6100000000f3 thread T0
    #0 0x6b0478  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #2 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #3 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #4 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #5 0x7f173ed37c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #6 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x6100000000f3 is located 0 bytes to the right of 179-byte region
[0x610000000040,0x6100000000f3)
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
Shadow bytes around the buggy address:
  0x0c207fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00[03]fa
  0x0c207fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8060: 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
==101583==ABORTING
```

## Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b0478)
```