⑂ **main** ▾   • • •

Poc / **otfcc** / **CVE-2022-35044.md**

🖼 **Cvjark** Create CVE-2022-35044.md   ⟳ **History**

👥 **1 contributor**

☰ 75 lines (65 sloc) │ 3.14 KB   • • •

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059909/id75_heap_buffer_overflow_sample_otfccdump%2B0x617087.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

```
==115405==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6070000000e0
at pc 0x000000617088 bp 0x7ffc10142fb0 sp 0x7ffc10142fa8
READ of size 1 at 0x6070000000e0 thread T0
    #0 0x617087  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x617087)
    #1 0x4feb66  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4feb66)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f93e83b7c86 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)

0x6070000000e0 is located 0 bytes to the right of 80-byte region
[0x607000000090,0x6070000000e0)
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 0x7f93e83b7c86 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+0x617087)
Shadow bytes around the buggy address:
  0x0c0e7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 04 fa fa fa
=>0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
  0x0c0e7fff8040: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8050: 00 00 00 fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0e7fff8060: fd fa fa fa fa fa 00 00 00 00 00 00 00 00 00 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
==115405==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x617087)
```