Cvjark / Poc Public

<> Code ⊙ Issues 1 Pull requests ▷ Actions Projects Security ···

main ▾ ···

Poc / otfcc / CVE-2022-35036.md

Cvjark Create CVE-2022-35036.md History

1 contributor

76 lines (66 sloc) | 3.22 KB ···

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059888/id18_heap_buffer_overflow_sample_otfccdump%2B0x6e1fc8.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

```
==106716==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000837
at pc 0x0000006e1fc9 bp 0x7fff2058d3a0 sp 0x7fff2058d398
READ of size 1 at 0x616000000837 thread T0
    #0 0x6e1fc8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e1fc8)
    #1 0x5eb5ec  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)
    #2 0x4fe227  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7fdfdc8c8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #5 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x616000000837 is located 685 bytes to the right of 522-byte region
[0x616000000380,0x61600000058a)
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 0x7fdfdc8c8c86 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+0x6e1fc8)
Shadow bytes around the buggy address:
  0x0c2c7fff80b0: 00 02 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2c7fff8100: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8150: 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
==106716==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e1fc8)
```