Cvjark Create CVE-2022-35043.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/9059903/id56_heap_buffer_overflow_sample_otfccdump%2B0x6c08a6.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

```
==113407==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f18b85fb808
at pc 0x0000006c08a7 bp 0x7ffe5e50c390 sp 0x7ffe5e50c388
READ of size 8 at 0x7f18b85fb808 thread T0
    #0 0x6c08a6  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c08a6)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f18bbbcac86 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)

0x7f18b85fb808 is located 8 bytes to the right of 1048576-byte region
[0x7f18b84fb800,0x7f18b85fb800)
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
    #1 0x526fd2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f18bbbcac86 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+0x6c08a6)
Shadow bytes around the buggy address:
  0x0fe3970b76b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3970b76f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe3970b7700: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7710: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7720: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7730: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7740: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3970b7750: 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
==113407==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c08a6)
```