Cvjark Create CVE-2022-35062.md History

1 contributor

92 lines (81 sloc) | 4.37 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059925/id134_heap_buffer_overflow_sample_otfccdump%2B0x6c0bc3.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

```
==104121==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x617000007110
at pc 0x0000006c0bc4 bp 0x7ffc16d4ecb0 sp 0x7ffc16d4eca8
READ of size 4 at 0x617000007110 thread T0
    #0 0x6c0bc3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0bc3)
    #1 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #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 0x7f987337ac86 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)

0x617000007110 is located 392 bytes to the right of 648-byte region
[0x617000006d00,0x617000006f88)
freed by thread T0 here:
    #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aeea8)
    #1 0x5add31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
    #2 0x540f73  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540f73)
    #3 0x6bc059  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bc059)
    #4 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #5 0x6baee8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6baee8)
    #6 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #7 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #8 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #9 0x7f987337ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x4aeea8 in realloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aeea8)
    #1 0x5add31  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5add31)
    #2 0x540696  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x540696)
    #3 0x6bda43  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6bda43)
    #4 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #5 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #6 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #7 0x7f987337ac86 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+0x6c0bc3)
Shadow bytes around the buggy address:
  0x0c2e7fff8dd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e7fff8de0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e7fff8df0: fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
=>0x0c2e7fff8e20: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8e70: 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
==104121==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0bc3)
```