Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / otfcc / CVE-2022-35054.md

Cvjark Create CVE-2022-35054.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/9059913/id82_heap_buffer_overflow_sample_otfccdump%2B0x6171b2.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

```
==116615==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000150
at pc 0x0000006171b3 bp 0x7ffccb343290 sp 0x7ffccb343288
READ of size 1 at 0x603000000150 thread T0
    #0 0x6171b2  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6171b2)
    #1 0x4febdc  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4febdc)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f9e1c28bc86 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)

0x603000000150 is located 0 bytes to the right of 32-byte region
[0x603000000130,0x603000000150)
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 0x7f9e1c28bc86 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+0x6171b2)
Shadow bytes around the buggy address:
  0x0c067fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c067fff8000: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8010: fd fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
=>0x0c067fff8020: 00 00 00 04 fa fa 00 00 00 00[fa]fa 00 00 04 fa
  0x0c067fff8030: fa fa 00 00 00 00 fa fa fd fd fd fa fa fa fd fd
  0x0c067fff8040: fd fa fa fa 00 00 06 fa fa fa fd fd fd fa fa fa
  0x0c067fff8050: 00 00 00 fa fa fa fd fd fd fd fa fa 00 00 02 fa
  0x0c067fff8060: fa fa 00 00 02 fa fa fa 00 00 02 fa fa fa 00 00
  0x0c067fff8070: 02 fa fa fa 00 00 02 fa fa fa 00 00 02 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
==116615==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6171b2)
```