Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / otfcc / CVE-2022-35049.md

Cvjark Create CVE-2022-35049.md History

1 contributor

75 lines (64 sloc) | 3.04 KB

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059905/id60_heap_buffer_overflow_sample_otfccdump%2B0x6b03b5.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

```
==114199==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000295
at pc 0x0000006b03b6 bp 0x7ffd165c5be0 sp 0x7ffd165c5bd8
READ of size 1 at 0x603000000295 thread T0
    #0 0x6b03b5  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b03b5)
    #1 0x6b99ca  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b99ca)
    #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 0x7f60e4d53c86 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)

0x603000000295 is located 0 bytes to the right of 21-byte region
[0x603000000280,0x603000000295)
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
    #1 0x6b536b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b03b5)
Shadow bytes around the buggy address:
  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 fd fd fd fa
  0x0c067fff8030: fa fa fd fd fd fa fa fa 00 00 06 fa fa fa fd fd
  0x0c067fff8040: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
=>0x0c067fff8050: 00 00[05]fa fa fa 00 00 00 fa fa fa fa fa fa fa
  0x0c067fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff80a0: 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
==114199==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b03b5)
```