Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / otfcc / CVE-2022-35058.md

Cvjark Create CVE-2022-35058.md History

1 contributor

74 lines (64 sloc) | 3.04 KB

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059921/id117_heap_buffer_overflow_sample_otfccdump%2B0x6b05ce.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

```
==102877==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000418
at pc 0x0000006b05cf bp 0x7ffe00e2fc60 sp 0x7ffe00e2fc58
READ of size 1 at 0x619000000418 thread T0
    #0 0x6b05ce  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05ce)
    #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 0x7fb14c4a8c86 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)

0x619000000418 is located 0 bytes to the right of 920-byte region
[0x619000000080,0x619000000418)
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+0x6b05ce)
Shadow bytes around the buggy address:
  0x0c327fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8080: 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff80d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==102877==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05ce)
```