Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / otfcc / CVE-2022-35066.md

Cvjark Create CVE-2022-35066.md History

1 contributor

74 lines (64 sloc) 3.05 KB

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059932/id188_heap_buffer_overflow_sample_otfccdump%2B0x6e41b8.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

```
==106312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x616000000ec2
at pc 0x0000006e41b9 bp 0x7fff002486b0 sp 0x7fff002486a8
WRITE of size 1 at 0x616000000ec2 thread T0
    #0 0x6e41b8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
    #1 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
    #2 0x4fbe60  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe60)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f5a9e97cc86 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)

0x616000000ec2 is located 0 bytes to the right of 578-byte region
[0x616000000c80,0x616000000ec2)
allocated by thread T0 here:
    #0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
    #1 0x6e3519  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e3519)
    #2 0x59ab0f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
Shadow bytes around the buggy address:
  0x0c2c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2c7fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2c7fff81d0: 00 00 00 00 00 00 00 00[02]fa fa fa fa fa fa fa
  0x0c2c7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8220: 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
==106312==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41b8)
```