

main

...

Poc / ofcc / CVE-2022-35059.md



Cvjark Create CVE-2022-35059.md

History

1 contributor



76 lines (66 sloc) | 3.22 KB

...

Product Link

<https://github.com/caryll/ofcc>

POC file

https://github.com/Cvjark/Poc/files/9059919/id110_heap_buffer_overflow_sample_otfccdump%2B0x6c0414.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

```
==102472==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fa28a7e5808
at pc 0x0000006c0415 bp 0x7ffe8b844290 sp 0x7ffe8b844288
READ of size 8 at 0x7fa28a7e5808 thread T0
#0 0x6c0414 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0414)
#1 0x527687 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
#2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
#3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
#4 0x7fa28e8f7c86 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)
```

0x7fa28a7e5808 is located 8 bytes to the right of 1048576-byte region
[0x7fa28a6e5800,0x7fa28a7e5800)
allocated by thread T0 here:

```
#0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
#1 0x526fd2 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x526fd2)
#2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
#3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
#4 0x7fa28e8f7c86 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+0x6c0414)

Shadow bytes around the buggy address:

```
0x0ff4d14f4ab0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff4d14f4ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff4d14f4ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff4d14f4ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0ff4d14f4af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff4d14f4b00: fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff4d14f4b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff4d14f4b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff4d14f4b30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff4d14f4b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0ff4d14f4b50: 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
==102472==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6c0414)
```