

main

...

Poc / ofcc / CVE-2022-35047.md



Cvjark Create CVE-2022-35047.md

History

1 contributor

74 lines (64 sloc) | 3.04 KB

...

Product Link

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

POC file

https://github.com/Cvjark/Poc/files/9059900/id41_heap_buffer_overflow_sample_otfccdump%2B0x6b05aa.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

```
==112565==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x608000000178
at pc 0x0000006b05ab bp 0x7fff844968e0 sp 0x7fff844968d8
READ of size 1 at 0x608000000178 thread T0
#0 0x6b05aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05aa)
#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 0x7f1fc338fc86 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)
```

0x608000000178 is located 0 bytes to the right of 88-byte region
[0x608000000120,0x608000000178)
allocated by thread T0 here:

```
#0 0x4aecdb in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecdb)
#1 0x6b536b (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b536b)
```

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05aa)

Shadow bytes around the buggy address:

```
0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
0x0c107fff8010: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00[fa]
0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c107fff8070: 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
==112565==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b05aa)
```