

main

...

Poc / ofcc / CVE-2022-35061.md



Cvjark Create CVE-2022-35061.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/9059927/id148_heap_buffer_overflow_sample_otfccdump%2B0x6e412a.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

```
==104506==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60800000017a
at pc 0x0000006e412b bp 0x7fff3383d690 sp 0x7fff3383d688
WRITE of size 1 at 0x60800000017a thread T0
#0 0x6e412a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e412a)
#1 0x59ab0f (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x59ab0f)
#2 0x4fbe96 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbe96)
#3 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
#4 0x7f034a2f9c86 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)
```

0x60800000017a is located 0 bytes to the right of 90-byte region
[0x608000000120,0x60800000017a)
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+0x6e412a)

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 fd fd fd fd fd fd fd fd fd fd fd
0x0c107fff8010: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 01
=>0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 02]
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
==104506==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e412a)
```