

main

...

Poc / ofcc / CVE-2022-35038.md



Cvjark Create CVE-2022-35038.md

History

1 contributor

78 lines (68 sloc) | 3.38 KB

...

Product Link

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

POC file

https://github.com/Cvjark/Poc/files/9059890/id23_heap_buffer_overflow_sample_otfccdump%2B0x6b064d.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

```
==108759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000000616
at pc 0x0000006b064e bp 0x7ffe8ca033c0 sp 0x7ffe8ca033b8
READ of size 1 at 0x612000000616 thread T0
#0 0x6b064d (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b064d)
#1 0x6b256a (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b256a)
#2 0x6b74c0 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b74c0)
#3 0x5265aa (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
#4 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
#5 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
#6 0x7f93b614bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
#7 0x41c549 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)
```

0x612000000616 is located 75 bytes to the right of 267-byte region
[0x6120000004c0,0x6120000005cb)
allocated by thread T0 here:

```
#0 0x4aecd8 in calloc (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4aecd8)
#1 0x6b69c5 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b69c5)
#2 0x4fe3fe (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
#3 0x4f5710 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
#4 0x7f93b614bc86 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+0x6b064d)

Shadow bytes around the buggy address:

```
0x0c247fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c247fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
0x0c247fff8090: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c247fff80a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c247fff80b0: 00 00 00 00 00 00 00 00 00 03 fa fa fa fa fa fa
=>0x0c247fff80c0: fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff8110: 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

==108759==ABORTING

Crash summary

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b064d)