Cvjark Create CVE-2022-35063.md History

1 contributor

74 lines (64 sloc) | 3.04 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059929/id170_heap_buffer_overflow_sample_otfccdump%2B0x6e41a8.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

```
==105392==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x611000030bc3
at pc 0x0000006e41a9 bp 0x7ffe6221d370 sp 0x7ffe6221d368
WRITE of size 1 at 0x611000030bc3 thread T0
    #0 0x6e41a8  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
    #1 0x5bea45  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)
    #2 0x4fbdd4  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbdd4)
    #3 0x4f5932  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #4 0x7f34f993dc86 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)

0x611000030bc3 is located 0 bytes to the right of 195-byte region
[0x611000030b00,0x611000030bc3)
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 0x5bea45  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5bea45)

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
Shadow bytes around the buggy address:
  0x0c227fffe120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c227fffe130: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c227fffe140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c227fffe150: fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c227fffe170: 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa fa
  0x0c227fffe180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fffe1c0: 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
==105392==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e41a8)
```