Cvjark Create CVE-2022-35039.md History

1 contributor

69 lines (60 sloc) | 2.72 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059894/id25_heap_buffer_overflow_sample_otfccdump%2B0x6e20a0.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

```
==109553==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6160000078a6
at pc 0x0000006e20a1 bp 0x7fffa376ea60 sp 0x7fffa376ea58
READ of size 1 at 0x6160000078a6 thread T0
    #0 0x6e20a0  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e20a0)
    #1 0x5eb5ec  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5eb5ec)
    #2 0x4fe227  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe227)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f2da0c05c86 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)

Address 0x6160000078a6 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e20a0)
Shadow bytes around the buggy address:
  0x0c2c7fff8ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ed0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2c7fff8f10: fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2c7fff8f60: 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
==109553==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6e20a0)
```