Cvjark Create CVE-2022-35021.md History

1 contributor

69 lines (60 sloc) | 2.9 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059942/id20_global-buffer-overflow_sample_1.zip

Command to reproduce

```
./otfccbuild --pretty [sample file] -o /dev/null
```

Product name & version

```
last github commit code : 617837b
```

Problem Type

```
global-buffer-overflow
```

Crash Detail

```
==15097==ERROR: AddressSanitizer: global-buffer-overflow on address
0x00000075fb88 at pc 0x000000718694 bp 0x7fffd615d380 sp 0x7fffd615d378
```

```
READ of size 4 at 0x00000075fb88 thread T0
    #0 0x718693  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
    #1 0x6f835d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6f835d)
    #2 0x4f5ad3  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5ad3)
    #3 0x7f69023d2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #4 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

0x00000075fb88 is located 56 bytes to the left of global variable 'cDigitsLut'
defined in '../../dep/extern/emyg-dtoa/emyg-dtoa.c:345:20' (0x75fbc0) of size 200
0x00000075fb88 is located 0 bytes to the right of global variable 'kPow10'
defined in '../../dep/extern/emyg-dtoa/emyg-dtoa.c:244:24' (0x75fb60) of size 40
SUMMARY: AddressSanitizer: global-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
Shadow bytes around the buggy address:
  0x0000800e3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f30: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9
  0x0000800e3f40: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000800e3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f60: 00 00 00 00 00 06 f9 f9 f9 f9 f9 f9 00 00 00 00
=>0x0000800e3f70: 00[f9]f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x0000800e3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3f90: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
  0x0000800e3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000800e3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==15097==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: global-buffer-overflow
(/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x718693)
```