Cvjark Create CVE-2022-35065.md History

1 contributor

37 lines (28 sloc) | 1.27 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059964/id196_SEGV_sample_otfccdump%2B0x65f724.zip

Command to reproduce

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

Product name & version

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

Problem Type

SEGV

Crash Detail

```
=================================================================
==1985==ERROR: AddressSanitizer: SEGV on unknown address 0x61b000010076 (pc
0x00000065f724 bp 0x7ffff2bcdf90 sp 0x7ffff2bcdde0 T0)
==1985==The signal is caused by a READ memory access.
    #0 0x65f724  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65f724)
    #1 0x4fe89d  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe89d)
    #2 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #3 0x7f4881d74c86 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)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x65f724)
==1985==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x65f724)
```