⑂ main ▾   •••

Poc / otfcc / **CVE-2022-35032.md**

Cvjark Create CVE-2022-35032.md   ⟲ History

⚇ **1 contributor**

☰ 40 lines (31 sloc) │ 1.42 KB   •••

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059962/id68_SEGV_sample_otfccdump%2B0x6b6a8f.zip

Command to reproduce

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

Product name & version

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

Problem Type

```
SEGV
```

Crash Detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==9840==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x0000006b6a8f bp 0x0c2600000041 sp 0x7ffdf341f950 T0)
==9840==The signal is caused by a READ memory access.
==9840==Hint: address points to the zero page.
    #0 0x6b6a8f  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6a8f)
    #1 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f4071149c86 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)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x6b6a8f)
==9840==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x6b6a8f)
```