Cvjark Create CVE-2022-35029.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/9059960/id58_SEGV_sample_otfccdump%2B0x6babea.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
=================================================================
==8370==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000704 (pc
0x0000006babea bp 0x7ffc00eb8610 sp 0x7ffc00eb82e0 T0)
==8370==The signal is caused by a READ memory access.
==8370==Hint: address points to the zero page.
    #0 0x6babea  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6babea)
    #1 0x527687  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x527687)
    #2 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f8358612c86 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+0x6babea)
==8370==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x6babea)
```