Cvjark Create CVE-2022-35031.md History

1 contributor

40 lines (31 sloc) | 1.52 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059963/id160_SEGV_sample_otfccdump%2B0x703969.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
=================================================================
==1585==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x000000703969 bp
0x7ffd74fa1170 sp 0x7ffd74f20f50 T0)
==1585==The signal is caused by a READ memory access.
==1585==Hint: this fault was caused by a dereference of a high value address (see
register values below).  Disassemble the provided pc to learn which register was
used.
    #0 0x703969  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x703969)
    #1 0x65be5b  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x65be5b)
    #2 0x4fe2f1  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe2f1)
    #3 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #4 0x7f72f8d40c86 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+0x703969)
==1585==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x703969)
```