

main

...

Poc / ofcc / CVE-2022-35028.md



Cvjark Create CVE-2022-35028.md

History

1 contributor



38 lines (29 sloc) | 1.26 KB

...

Product Link

<https://github.com/caryll/ofcc>

POC file

https://github.com/Cvjark/Poc/files/9059957/id33_SEGV_sample_otfccdump%2B0x4fbbb6.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

```
=====
==2966==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000036 (pc
0x0000004fbbb6 bp 0x7ffddb299ed0 sp 0x7ffddb299da0 T0)
==2966==The signal is caused by a READ memory access.
==2966==Hint: address points to the zero page.
    #0 0x4fbbb6 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fbbb6)
    #1 0x4f5932 (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5932)
    #2 0x7f3e141cac86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #3 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+0x4fbbb6)
==2966==ABORTING

Crash summary

SUMMARY: AddressSanitizer: SEGV (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4fbbb6)