Cvjark Create CVE-2022-35023.md History

1 contributor

48 lines (39 sloc) | 1.78 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059947/id4_SEGV_sample_libc6_%2B0xbb384.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
  =================================================================
```

```
==6233==ERROR: AddressSanitizer: SEGV on unknown address 0x6120002ad5dd (pc
0x7fbef8354384 bp 0x7ffecdbe0f10 sp 0x7ffecdbe06a8 T0)
==6233==The signal is caused by a READ memory access.
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: failed to fork (errno 12)
==6233==WARNING: Failed to use and restart external symbolizer!
    #0 0x7fbef8354384  (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
    #1 0x4ad6eb  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4ad6eb)
    #2 0x6b53ed  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
    #3 0x6b6d86  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6d86)
    #4 0x5265aa  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x5265aa)
    #5 0x4fe3fe  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4fe3fe)
    #6 0x4f5710  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x4f5710)
    #7 0x7fbef82bac86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #8 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
==6233==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
```