Cvjark Create CVE-2022-35024.md History

1 contributor

42 lines (33 sloc) | 1.75 KB ...

Product Link

https://github.com/caryll/otfcc

POC file

https://github.com/Cvjark/Poc/files/9059952/id10_SEGV_sample_memmove-vec-unaligned-erms.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
=================================================================
==128856==ERROR: AddressSanitizer: SEGV on unknown address 0x612000096e63 (pc
0x7fdeb5ff1384 bp 0x7ffd479c81d0 sp 0x7ffd479c7968 T0)
==128856==The signal is caused by a READ memory access.
    #0 0x7fdeb5ff1384  /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:431
    #1 0x4ad6eb in __asan_memcpy (/home/bupt/Desktop/otfcc/bin/release-
x64/otfccdump+0x4ad6eb)
    #2 0x6b53ed  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b53ed)
    #3 0x6b6b99  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x6b6b99)
    #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 0x7fdeb5f57c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #8 0x41c549  (/home/bupt/Desktop/otfcc/bin/release-x64/otfccdump+0x41c549)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:431
==128856==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:431
```