New issue

Jump to bottom

AddressSanitizer: SEGV /build/glibc-sMfBJT/glibc-2.31/string/../sysdeps/x86_64/multiarch/strlen-avx2.S:65 #691

Closed p870613 opened this issue on Apr 10 · 1 comment

p870613 commented on Apr 10

SUMMARY: AddressSanitizer: SEGV /build/glibc-sMfBJT/glibc-2.31/string/../sysdeps/x86_64/multiarch/strlen-avx2.S:65

- Version

```
➜  mp42hls_test git:(master) ✗ ./mp42hls
MP4 To HLS File Converter - Version 1.2
(Bento4 Version 1.6.0.0)
(c) 2002-2018 Axiomatic Systems, LLC
```

branch `4d8e1fc`

- Platform

```
➜   gcc --version
gcc (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
Copyright (C) 2017 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

➜   uname -r
5.4.0-91-generic
➜  lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic
```

- Steps to reproduce

```
mkdir build
cd build
cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -
DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address" -DCMAKE_MODULE_LINKER_FLAGS="-fsanitize=address"
make
./mp42hls   --encryption-iv-mode fps ./poc
```

- Asan

```
➜  build git:(master) ✗ ./mp42hls   --encryption-iv-mode fps ./poc
AddressSanitizer:DEADLYSIGNAL
=================================================================
==15594==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fd9e20834e5 bp
0x7ffe2c690150 sp 0x7ffe2c68f8c8 T0)
==15594==The signal is caused by a READ memory access.
==15594==Hint: address points to the zero page.
    #0 0x7fd9e20834e4  (/lib/x86_64-linux-gnu/libc.so.6+0x18b4e4)
    #1 0x7fd9e249c8fb  (/lib/x86_64-linux-gnu/libasan.so.5+0x678fb)
    #2 0x557f40b2b5f3 in main /home/lin/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:1853
    #3 0x7fd9e1f1f0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #4 0x557f40b1f96d in _start (/home/lin/Bento4/build/mp42hls+0x32b96d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x18b4e4)
==15594==ABORTING
```

poc: poc.zip

Thanks !!

barbibulle closed this as completed in `33331ce` on May 1

---

p870613 commented on May 17 — Author

Assigned CVE-2022-29017

CastagnaIT pushed a commit to xbmc/Bento4 that referenced this issue on Jul 3

`fix axiomatic-systems#691` 23cb941

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant