New issue

Jump to bottom

SEGV at moddable/xs/sources/xsCommon.c:916 #440

Closed **kvenux** opened this issue on Sep 4, 2020 · 0 comments

Labels confirmed fixed - please verify

kvenux commented on Sep 4, 2020

Build environment:

Ubuntu 16.04
gcc 5.4.0
xst version: 5639abb
build command:
cd /path/to/moddable/xs/makefiles/lin
make
test command: ./xst poc

Target device:

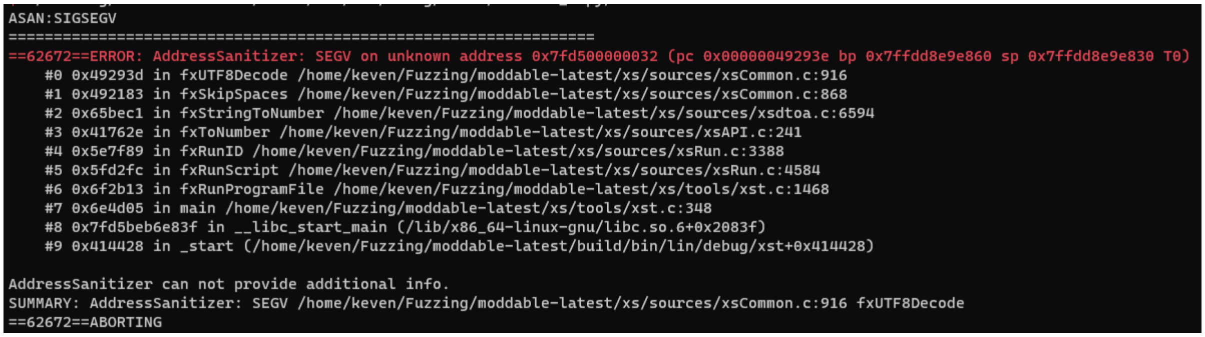
Desktop Linux

POC

xs-000271.txt

Description

Below is the ASAN outputs.



```
ASAN:SIGSEGV
=================================================================
==62672==ERROR: AddressSanitizer: SEGV on unknown address 0x7fd500000032 (pc 0x00000049293e bp 0x7ffdd8e9e860 sp 0x7ffdd8e9e830 T0)
    #0 0x49293d in fxUTF8Decode /home/keven/Fuzzing/moddable-latest/xs/sources/xsCommon.c:916
    #1 0x492183 in fxSkipSpaces /home/keven/Fuzzing/moddable-latest/xs/sources/xsCommon.c:868
    #2 0x65bec1 in fxStringToNumber /home/keven/Fuzzing/moddable-latest/xs/sources/xsdtoa.c:6594
    #3 0x41762e in fxToNumber /home/keven/Fuzzing/moddable-latest/xs/sources/xsAPI.c:241
    #4 0x5e7f89 in fxRunID /home/keven/Fuzzing/moddable-latest/xs/sources/xsRun.c:3388
    #5 0x5fd2fc in fxRunScript /home/keven/Fuzzing/moddable-latest/xs/sources/xsRun.c:4584
    #6 0x6f2b13 in fxRunProgramFile /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:1468
    #7 0x6e4d05 in main /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:348
    #8 0x7fd5beb6e83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #9 0x414428 in _start (/home/keven/Fuzzing/moddable-latest/build/bin/lin/debug/xst+0x414428)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/keven/Fuzzing/moddable-latest/xs/sources/xsCommon.c:916 fxUTF8Decode
==62672==ABORTING
```

kvenux changed the title ~~SEGV at moddable/xs/sources/xsCommon.c:868~~ SEGV at moddable/xs/sources/xsCommon.c:916 on Sep 4, 2020

phoddie added the confirmed label on Sep 4, 2020

mkellner pushed a commit that referenced this issue on Sep 8, 2020

XS: #440 404c84d

phoddie added the fixed - please verify label on Sep 8, 2020

kvenux closed this as completed on Sep 8, 2020

Assignees
No one assigned

Labels
confirmed fixed - please verify

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

2 participants