New issue

Jump to bottom

SEGV at moddable/xs/sources/xsProxy.c:171 #441

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-000230.txt

Description

Below is the ASAN outputs.

```
ASAN:SIGSEGV
=================================================================
==11351==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000058e995 bp 0x7ffd35163ae0 sp 0x7ffd35163ac0 T0)
    #0 0x58e994 in fxProxyGetter /home/keven/Fuzzing/moddable-latest/xs/sources/xsProxy.c:171
    #1 0x5b57ec in fxRunID /home/keven/Fuzzing/moddable-latest/xs/sources/xsRun.c:767
    #2 0x4d9153 in fx_Function_prototype_apply /home/keven/Fuzzing/moddable-latest/xs/sources/xsFunction.c:358
    #3 0x5b57ec in fxRunID /home/keven/Fuzzing/moddable-latest/xs/sources/xsRun.c:767
    #4 0x5fd2fc in fxRunScript /home/keven/Fuzzing/moddable-latest/xs/sources/xsRun.c:4584
    #5 0x6f2b13 in fxRunProgramFile /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:1468
    #6 0x6e4d05 in main /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:348
    #7 0x7f2aff34b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #8 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/xsProxy.c:171 fxProxyGetter
==11351==ABORTING
```

kvenux changed the title ~~SEGV at moddable/xs/sources/xsRun.c:767~~ SEGV at moddable/xs/sources/xsProxy.c:171 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: #441 644d63b

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