

New issue

Jump to bottom

SEGV at moddable/xs/sources/xsSyntactical.c:3419 #442

🔒 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-000425.txt](#)

Description

Below is the ASAN outputs.

```
ASAN:SIGSEGV
=====
==118063==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000002 (pc 0x000000638294 bp 0x7fff5f793b90 sp 0x7fff5f793b50 T0)
#0 0x638293 in fxObjectBindingFromExpression /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:3419
#1 0x639979 in fxCheckReference /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:3601
#2 0x629b1b in fxForStatement /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:1387
#3 0x628524 in fxStatement /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:1180
#4 0x627e99 in fxBody /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:1097
#5 0x627914 in fxProgram /home/keven/Fuzzing/moddable-latest/xs/sources/xsSyntactical.c:1065
#6 0x63d6f7 in fxParserTree /home/keven/Fuzzing/moddable-latest/xs/sources/xsTree.c:168
#7 0x5742ff in fxLoadScript /home/keven/Fuzzing/moddable-latest/xs/sources/xsPlatforms.c:388
#8 0x6f295b in fxRunProgramFile /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:1466
#9 0x6e4d05 in main /home/keven/Fuzzing/moddable-latest/xs/tools/xst.c:348
#10 0x7efc6a1c983f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#11 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/xsSyntactical.c:3419 fxObjectBindingFromExpression
==118063==ABORTING
```


 phoddie added the **confirmed** label on Sep 4, 2020

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

[XS: #442](#)

38c815c

 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

