Moddable-OpenSource / **moddable** Public

Code Issues 25 Pull requests 15 Discussions Actions Projects ···

New issue

Jump to bottom

Heap buffer overflow at moddable/xs/sources/xsSyntaxical.c:3562 #432

Closed **kvenux** opened this issue on Aug 31, 2020 · 2 comments

Labels **confirmed** fixed - please verify

kvenux commented on Aug 31, 2020

Build environment:

Ubuntu 16.04
gcc 5.4.0
xst version: `de64c70` (git hash)
build command:
cd /path/to/moddable/xs/makefiles/lin
make
test command: ./xst poc

Target device:

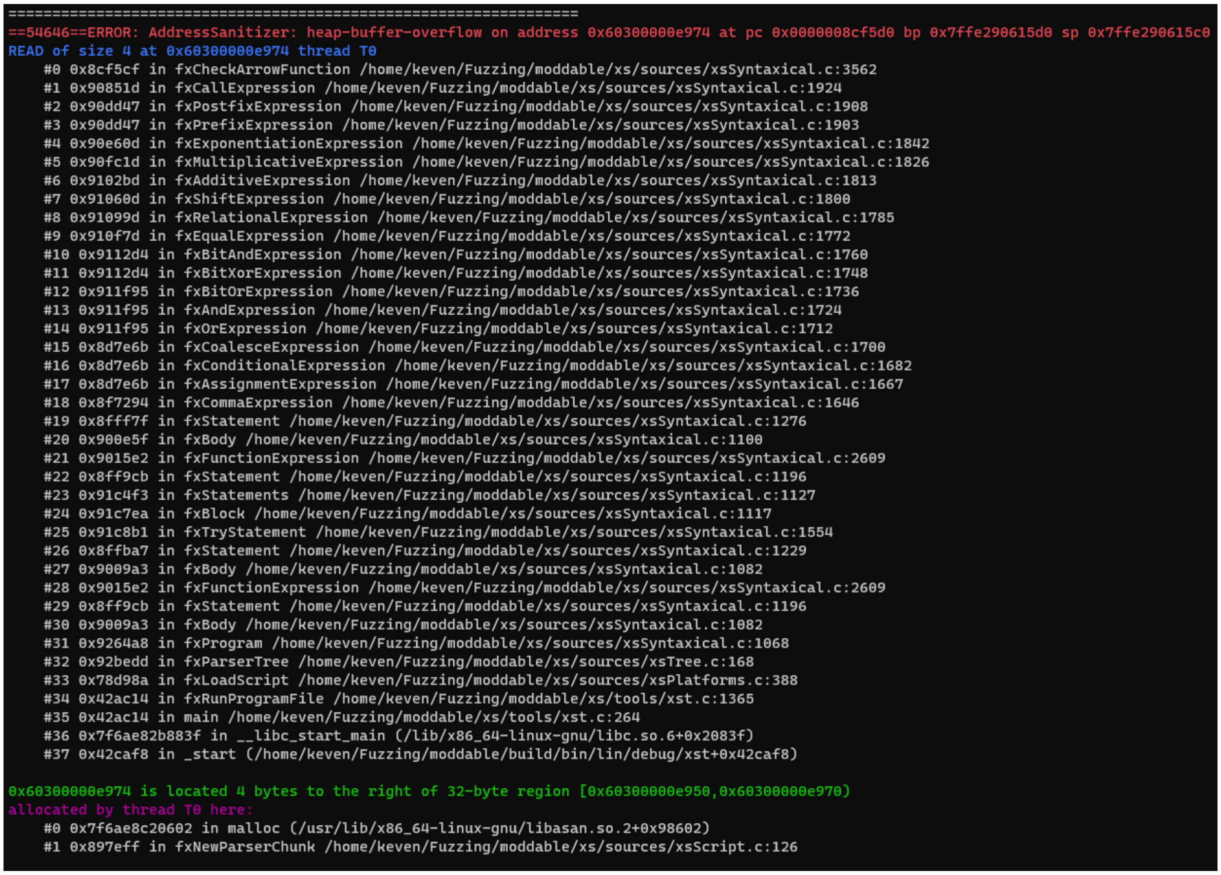
Desktop Linux

POC

000053.txt

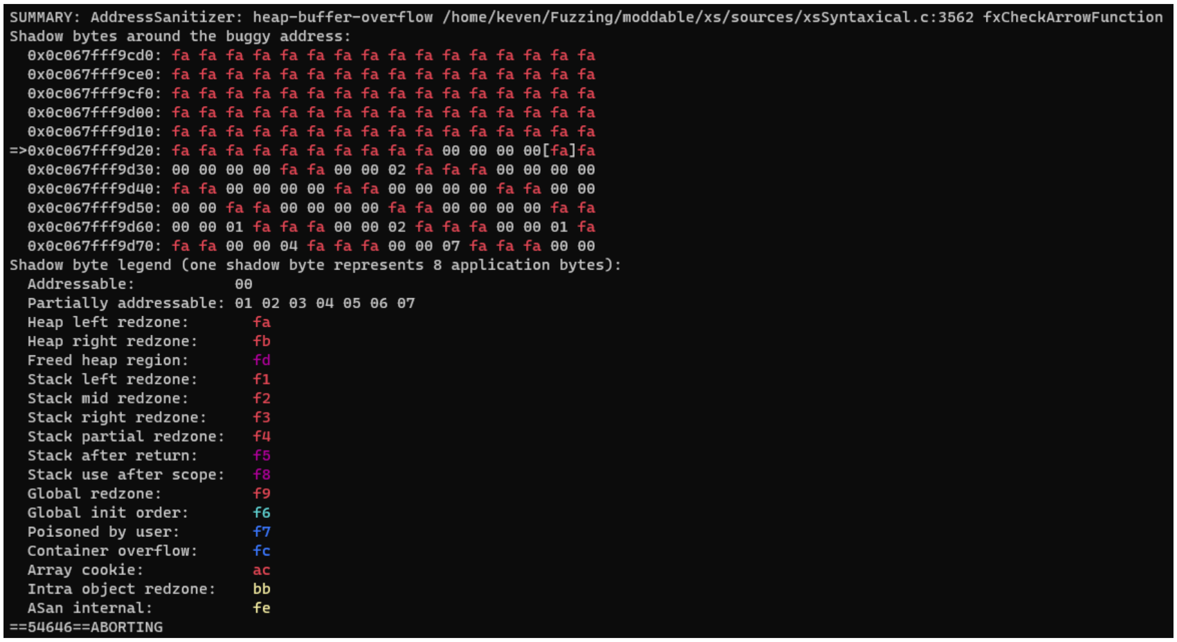
Description

Below is the ASAN outputs. Heap buffer overflow at moddable/xs/sources/xsSyntaxical.c:3562



```
=================================================================
==54646==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000e974 at pc 0x0000008cf5d0 bp 0x7ffe290615d0 sp 0x7ffe290615c0
READ of size 4 at 0x60300000e974 thread T0
    #0 0x8cf5cf in fxCheckArrowFunction /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:3562
    #1 0x90851d in fxCallExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1924
    #2 0x90dd47 in fxPostfixExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1908
    #3 0x90dd47 in fxPrefixExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1903
    #4 0x90e60d in fxExponentiationExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1842
    #5 0x90fc1d in fxMultiplicativeExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1826
    #6 0x9102bd in fxAdditiveExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1813
    #7 0x91060d in fxShiftExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1800
    #8 0x91099d in fxRelationalExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1785
    #9 0x910f7d in fxEqualExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1772
    #10 0x9112d4 in fxBitAndExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1760
    #11 0x9112d4 in fxBitXorExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1748
    #12 0x911f95 in fxBitOrExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1736
    #13 0x911f95 in fxAndExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1724
    #14 0x911f95 in fxOrExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1712
    #15 0x8d7e6b in fxCoalesceExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1700
    #16 0x8d7e6b in fxConditionalExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1682
    #17 0x8d7e6b in fxAssignmentExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1667
    #18 0x8f7294 in fxCommaExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1646
    #19 0x8fff7f in fxStatement /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1276
    #20 0x900e5f in fxBody /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1100
    #21 0x9015e2 in fxFunctionExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:2609
    #22 0x8ff9cb in fxStatement /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1196
    #23 0x91c4f3 in fxStatements /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1127
    #24 0x91c7ea in fxBlock /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1117
    #25 0x91c8b1 in fxTryStatement /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1554
    #26 0x8ffba7 in fxStatement /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1229
    #27 0x9009a3 in fxBody /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1082
    #28 0x9015e2 in fxFunctionExpression /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:2609
    #29 0x8ff9cb in fxStatement /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1196
    #30 0x9009a3 in fxBody /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1082
    #31 0x9264a8 in fxProgram /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:1068
    #32 0x92bedd in fxParserTree /home/keven/Fuzzing/moddable/xs/sources/xsTree.c:168
    #33 0x78d98a in fxLoadScript /home/keven/Fuzzing/moddable/xs/sources/xsPlatforms.c:388
    #34 0x42ac14 in fxRunProgramFile /home/keven/Fuzzing/moddable/xs/tools/xst.c:1365
    #35 0x42ac14 in main /home/keven/Fuzzing/moddable/xs/tools/xst.c:264
    #36 0x7f6ae82b883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #37 0x42caf8 in _start (/home/keven/Fuzzing/moddable/build/bin/lin/debug/xst+0x42caf8)

0x60300000e974 is located 4 bytes to the right of 32-byte region [0x60300000e950,0x60300000e970)
allocated by thread T0 here:
    #0 0x7f6ae8c20602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x897eff in fxNewParserChunk /home/keven/Fuzzing/moddable/xs/sources/xsScript.c:126
```



```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/keven/Fuzzing/moddable/xs/sources/xsSyntaxical.c:3562 fxCheckArrowFunction
Shadow bytes around the buggy address:
  0x0c067fff9cd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9ce0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9cf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9d00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9d10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c067fff9d20: fa fa fa fa fa fa fa fa fa fa 00 00 00 00[fa]fa
  0x0c067fff9d30: 00 00 00 00 fa fa 00 00 02 fa fa fa 00 00 00 00
  0x0c067fff9d40: fa fa 00 00 00 00 fa fa 00 00 00 00 fa fa 00 00
  0x0c067fff9d50: 00 00 fa fa 00 00 00 00 fa fa 00 00 00 00 fa fa
  0x0c067fff9d60: 00 00 01 fa fa fa 00 00 02 fa fa fa 00 00 01 fa
  0x0c067fff9d70: fa fa 00 00 04 fa fa fa 00 00 07 fa fa fa 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==54646==ABORTING
```

phoddie added confirmed question cannot reproduce and removed question cannot reproduce labels on Aug 31, 2020

phoddie commented on Aug 31, 2020 Collaborator

The provided script may be reduced to the following:

```
function v4 = ()(v6, v7) {
}
```

❤️ 1

kvenux commented on Sep 1, 2020 Author

> The provided script may be reduced to the following:

> ```
> function v4 = ()(v6, v7) {
> }
> ```

Great. I have checked. This test case can be trimmed in this way.

mkellner pushed a commit that referenced this issue on Sep 3, 2020

`XS: #432` df143cb

mkellner pushed a commit that referenced this issue on Sep 3, 2020

`XS: #432 sanitized` 9184666

phoddie added the fixed - please verify label on Sep 3, 2020

kvenux closed this as completed on Sep 4, 2020

Assignees

No one assigned

Labels

confirmed fixed - please verify

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants