<> Code ○ Issues 27

11 Pull requests 15 Discussions (Actions Projects

Jump to bottom New issue

stack-overflow(fxBinaryExpressionNodeDistribute) #587

⊙ Closed rain6851 opened this issue on Feb 26, 2021 · 2 comments

Labels

fixed - please verify

```
rain6851 commented on Feb 26, 2021
```

Enviroment

```
operating system: ubuntu18.04
compile command: cd /pathto/moddable/xs/makefiles/lin
test command: ./xst poc
```

poc:

```
function getHiddenValue() {
      oob = oob.replace('', '-0'.repeat(1048576));
      var str = '(new Number(-0))' + oob + '(new Boolean(false))';
var fun = eval(str);
      Object.assign(obj, fun);
      return obj;
function makeOobString() {
   var hiddenValue = getHiddenValue();
     var numerivatue = gerniodenvalue
var str = '-Infinity';
var fun = eval(str);
Object.assign(fun, hiddenValue);
var oobString = fun.toString();
      return oobString;
var oobString = makeOobString();
```

description

```
==6025==ERROR: AddressSanitizer: stack-overflow on address 0x7fff6d476ff8 (pc 0x000000646053 bp 0x7fff6d477020 sp 0x7fff6d476ff0 T0)
    #0 0x646052 in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:265
    #1 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #2 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #3 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #4 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #5 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #6 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #7 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#8 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #9 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#10 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #11 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#12 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #13 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #14 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #15 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #16 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #17 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #18 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #19 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #20 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:361
    #21 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #24 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #25 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #26 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #27 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/ms/sources/xsTree.c:267 #28 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/ms/sources/xsScope.c:355
    #29 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#30 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#31 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #32 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #33 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #34 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #35 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
    #36 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #37 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
    #38 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #39 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
    #40 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #41 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
```

#42 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #43 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #44 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361

```
#46 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#47 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:361
#48 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #49 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#50 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #51 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#52 0x607h7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#53 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#54 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#55 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #56 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#58 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#59 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #60 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#61 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#62 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#63 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#64 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#65 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:361
#66 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#68 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #69 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#70 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#71 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#72 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#73 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#74 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #75 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#76 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#77 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #78 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#79 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355 #80 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:361
#81 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#82 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#83 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #84 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#85 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#86 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#87 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#88 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #89 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#90 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #91 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#92 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #93 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#94 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#95 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #96 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#97 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#98 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #99 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#100 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#101 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #102 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#103 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#104 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#105 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#106 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#107 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#108 0x64609b in fxBinaryExpressionNodeDistribute /home/nodemmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #109 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#110 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#111 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#112 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#113 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#114 0x64609b in fxBinaryExpressionNodeDistribute /home/nodemmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #115 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#116 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#117 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#118 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#119 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #120 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#121 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#122 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#123 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#124 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#125 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#126 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#127 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#128 0x60fc2l in fxNbdeDispatchHoist /home/node/mmfuzzer/asan_moddable/ms/sycurces/xsScope.c:361
#129 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#130 0x607b7f in fxNodehoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #131 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#132 0x64609b in fxBinaryExpressionNodeDistribute /home/nodemmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267  
#133 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#134 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #135 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#136 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#137 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#138 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#139 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#140 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#141 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#142 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#143 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #144 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#145 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#146 0x60fc21 in fxNbdeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #147 0x60fc09b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#148 0x607b7f in fxNodehoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #149 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#150 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#151 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#152 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #153 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#154 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#156 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#157 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
```

#158 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361

```
#159 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#160 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#161 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #162 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#163 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #164 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#165 0x64609h in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#166 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#167 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#168 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #169 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#170 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #171 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#172 0x60707bf in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#173 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#174 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:267
#175 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#176 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #177 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/: #178 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#179 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #180 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#181 0x607b7f in fxNodehoist /home/node/mmfuzzer/asan_moddable/msddable/xs/sources/xsScope.c:355 #182 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:361
#183 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#184 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#185 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#186 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#187 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#188 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #189 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#190 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #191 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#192 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/ms/ssources/xsTree.c:267
#193 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#194 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #195 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#196 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#197 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #198 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#199 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#200 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #201 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #202 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#203 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xxScope.c:361 #204 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#205 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#206 0x607c21 in fxNodeDispatchHoist //home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #207 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:267
#208 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #209 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#210 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#211 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#212 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #213 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#214 0x607b7f in fxNodehoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #215 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#216 0x64609b in fxBinaryExpressionNodeDistribute /home/nodemmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #217 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#218 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#219 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#220 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#221 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #222 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#223 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#224 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#225 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#226 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#227 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #228 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#229 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#230 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#231 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#232 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355 #233 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#234 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#235 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#236 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #237 0x64600b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#238 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#239 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#240 0x64609b in fxBinarvExpressionNodeDistribute /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsTree.c:267
#241 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#242 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#243 0x64609b in fxBinaryExpressionNodeDistribute /home/nodemmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267 #244 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/xs/sources/xsScope.c:355
#245 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361 #246 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#247 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:355
#248 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361
#249 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267
#250 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355
#251 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan moddable/moddable/xs/sources/xsScope.c:361
```

SUMMARY: AddressSanitizer: stack-overflow /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:265 fxBinaryExpressionNodeDistribute ==6025==ABORTING

dckc mentioned this issue on Mar 2, 2021

arguing the security properties of xsnap (XS, SES, JS) Agoric/agoric-sdk#2224



dckc commented on Mar 5, 2021

Hi @rain6851 this is great work!

I tried to do something similar back in January... Agoric/agoric-sdk#2224 (comment)

but I didn't get very far. I would really appreciate your help understanding how to do this and learning about your fuzzing projects. Any chance you're available to discuss it with me some time? Feel free to write to me offline at dckc@madmode.com or via keybase chat: https://keybase.io/dckc

rain6851 commented on Mar 6, 2021

Author

Hi @rain6851 this is great work!

I tried to do something similar back in January... Agoric/agoric-sdk#2224 (comment)

but I didn't get very far. I would really appreciate your help understanding how to do this and learning about your fuzzing projects. Any chance you're available to discuss it with me some time? Feel free to write to me offline at dckc@madmode.com or via keybase chat: https://keybase.io/dckc

Related technologies will be published in the form of papers. Please help me apply for a CVE number to encourage me.

 \Box mkellner pushed a commit that referenced this issue on Mar 15, 2021

XS: #586 & #587 dbd3a5f

phoddie added the fixed - please verify label on Mar 15, 2021

phoddie closed this as completed on Mar 23, 2021

Assignees

No one assigned

Labels

fixed - please verify

Projects

None ye

Milestone

No milestone

Development

No branches or pull requests

3 participants

