

New issue

[Jump to bottom](#)

stack-overflow #586



rain6851 opened this issue on Feb 26, 2021 · 0 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('', '.*'.repeat(1048576));
  var str = '[1]' + oob + '>';
  var t2 = [
    4,
    4,
    4
  ];
  var fun = eval(str);
  var y = 0;
  Object.assign(obj, fun);
  return obj;
}

function makeOobString() {
  var hiddenValue = getHiddenValue();
  var str = 'class x extends Array{}';
  var fun = eval(str);
  var temp = [];
  Object.assign(fun, hiddenValue);
  var oobString = fun.toString();
  return oobString;
}

var oobString = makeOobString();
```



description

ASAN:SIGSEGV

```
=====
==5984==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd44d69ff0 (pc 0x7f238c4be26e bp 0x000000000028 sp 0x7ffd44d69fe0 T0)
#0 0x7f238c4be26d (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xb026d)
#1 0x7f238c4bdd67 (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xafd67)
#2 0x7f238c430f4f (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x22f4f)
#3 0x7f238c4a65d2 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x985d2)
#4 0x61189b in fxNewParserChunk /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScript.c:126
#5 0x611994 in fxNewParserChunkClear /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsScript.c:137
#6 0x62be05 in fxPushNodeStruct /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:595
#7 0x63703c in fxLiteralExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:2256
#8 0x634d11 in fxCallExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1951
#9 0x634aa1 in fxPostfixExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1938
#10 0x634a86 in fxPrefixExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1933
#11 0x63444b in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1872
#12 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#13 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#14 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#15 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#16 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#17 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#18 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#19 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#20 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#21 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#22 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#23 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#24 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#25 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#26 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#27 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#28 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#29 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#30 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#31 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#32 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#33 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#34 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#35 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#36 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#37 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
#38 0x6344f6 in fxExponentiationExpression /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsSyntactical.c:1877
```

[illegible]

[illegible]

  **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

2 participants

