New issue

Jump to bottom

Heap-buffer-overflow in ecma_utf8_string_to_number_by_radix (ecma-helpers-conversion.c) #4882

Closed **hope-fly** opened this issue on Dec 9, 2021 · 3 comments

hope-fly commented on Dec 9, 2021 • edited

JerryScript revision

Commit: 51da1551

Version: v3.0.0

Build platform

Ubuntu 18.04.5 LTS (Linux 5.4.0-44-generic x86_64)

Build steps

```
./tools/build.py --clean --debug --profile=es2015-subset --compile-flag=-fsanitize=address --compile-
```

Test case

```
function JSEtest(val) {
  return Number(val);
}

isNaN(JSEtest("+0x0"));
isNaN(JSEtest("+0xFF"));
isNaN(JSEtest("-0xFF"));
```

Execution steps & Output

```
$ ./jerryscript/build/bin/jerry poc.js

=================================================================
==103276==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xf5d005de at pc 0x566a6771 bp 0xf
READ of size 1 at 0xf5d005de thread T0
    #0 0x566a6770 in ecma_utf8_string_to_number_by_radix /root/jerryscript/jerry-core/ecma/base/ecma-
    #1 0x566a7a09 in ecma_utf8_string_to_number /root/jerryscript/jerry-core/ecma/base/ecma-helpers-c
    #2 0x566bacc7 in ecma_string_to_number /root/jerryscript/jerry-core/ecma/base/ecma-helpers-string
    #3 0x5673c738 in ecma_op_to_numeric /root/jerryscript/jerry-core/ecma/operations/ecma-conversion.
    #4 0x568bb03b in ecma_builtin_number_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-obje
    #5 0x56706f7c in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ecm
    #6 0x567488b4 in ecma_op_function_call_native_built_in /root/jerryscript/jerry-core/ecma/operatio
    #7 0x5674ea1d in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function
    #8 0x5674ea1d in ecma_op_function_validated_call /root/jerryscript/jerry-core/ecma/operations/ecm
    #9 0x56877f5e in opfunc_call /root/jerryscript/jerry-core/vm/vm.c:762
    #10 0x56877f5e in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5266
    #11 0x5687be7c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5363
    #12 0x56748101 in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-
    #13 0x5674ea3d in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-functio
    #14 0x5674ea3d in ecma_op_function_validated_call /root/jerryscript/jerry-core/ecma/operations/ec
    #15 0x56877f5e in opfunc_call /root/jerryscript/jerry-core/vm/vm.c:762
    #16 0x56877f5e in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5266
    #17 0x5687adb8 in vm_run /root/jerryscript/jerry-core/vm/vm.c:5363
    #18 0x5687adb8 in vm_run_global /root/jerryscript/jerry-core/vm/vm.c:290
    #19 0x5666d94f in jerry_run /root/jerryscript/jerry-core/api/jerryscript.c:533
    #20 0x56653d23 in main /root/jerryscript/jerry-main/main-jerry.c:169
    #21 0xf76fff20 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18f20)
    #22 0x5665d359  (/root/jerryscript/build/bin/jerry+0x3b359)

0xf5d005de is located 0 bytes to the right of 14-byte region [0xf5d005d0,0xf5d005de)
allocated by thread T0 here:
    #0 0xf7aaaf54 in malloc (/usr/lib32/libasan.so.4+0xe5f54)
    #1 0x5665af4c in jmem_heap_alloc /root/jerryscript/jerry-core/jmem/jmem-heap.c:254
    #2 0x5665af4c in jmem_heap_gc_and_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:291
    #3 0x5665af4c in jmem_heap_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:324

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/jerryscript/jerry-core/ecma/base/ecma-helpers-c
Shadow bytes around the buggy address:
  0x3eba0060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x3eba0070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x3eba0080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x3eba0090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x3eba00a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x3eba00b0: fa fa fa fa fa fa fa fa fa fa 00[06]fa fa fd fd
  0x3eba00c0: fa fa 05 fa fa fa 00 00 fa fa 00 00 fa fa 05 fa
  0x3eba00d0: fa fa fd fa fa fa fd fa fa fa 00 04 fa fa fd fd
  0x3eba00e0: fa fa fd fd fa fa 00 00 fa fa 00 06 fa fa 00 03
  0x3eba00f0: fa fa 00 07 fa fa 00 00 fa fa fa fa fa fa fa fa
  0x3eba0100: 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
  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
==103276==ABORTING
```

Credits: Found by OWL337 team.

hope-fly commented on Dec 9, 2021 • edited Author

Another form of PoC

```
function JSEtest_Int(str) {
  return str | 0;
}

function JSEtest_Dbl(str) {
  return str * 1.5;
}

JSEtest_Int("0x10");
JSEtest_Int("-0x10");

JSEtest_Dbl("0x10");
JSEtest_Dbl("-0x10");
```

rerobika commented on Dec 9, 2021 Member

Closed via #4850, please always use the latest master

👍 2

 **rerobika** closed this as completed on Dec 9, 2021

hope-fly commented on Dec 9, 2021 • edited ▾ Author

Okay, I found this bug two days ago but forgot to report until today. If it's right, pls label it!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants