

New issue

Jump to bottom

heap-buffer-overflow in lexer_parse_number #4442

Closed owl337 opened this issue on Jan 11, 2021 · 0 comments · Fixed by #4448

Assignees



Labels

bug

owl337 commented on Jan 11, 2021

JerryScript revision

fdaacde

Build platform

Ubuntu 18.04.5 LTS(Linux 4.15.0-119-generic x86_64)

Build steps

```
./tools/build.py --clean --debug --compile-flag=-fsanitize=address \
--compile-flag=-m32 --compile-flag=-fno-omit-frame-pointer \
--compile-flag=-fno-common --compile-flag=-g --strip=off \
--system-allocator=on --logging=on --linker-flag=-fuse-lld=gold \
--error-messages=on --profile=es2015-subset
```

Test case

```
eval('0x100000000');
```

Output

```
=====
==15467==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xf5b00925 at pc 0x5673c8d4 bp 0xffe81f18 sp 0xffe81f08
READ of size 1 at 0xf5b00925 thread T0
#0 0x5673c8d3 in lexer_parse_number /root/jerryscript/jerry-core/parser/js/js-lexer.c:1396
#1 0x5673da94 in lexer_next_token /root/jerryscript/jerry-core/parser/js/js-lexer.c:1662
#2 0x566c3e07 in scanner_scan_all /root/jerryscript/jerry-core/parser/js/js-scanner.c:2518
#3 0x566a657a in parser_parse_source /root/jerryscript/jerry-core/parser/js/js-parser.c:1896
#4 0x566abd30 in parser_parse_script /root/jerryscript/jerry-core/parser/js/js-parser.c:2806
#5 0x5665fe7c in ecma_op_eval_chars_buffer /root/jerryscript/jerry-core/ecma/operations/ecma-eval.c:99
#6 0x5665fc4e in ecma_op_eval /root/jerryscript/jerry-core/ecma/operations/ecma-eval.c:58
#7 0x5670d998 in ecma_builtin_global_object_eval /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-global.c:110
#8 0x5670f33a in ecma_builtin_global_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-global.c:607
#9 0x5663f710 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1490
#10 0x5663f9a6 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1522
#11 0x56663e87 in ecma_op_function_call_native /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1246
#12 0x56664810 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1416
#13 0x566de64b in opfunc_call /root/jerryscript/jerry-core/vm/vm.c:822
#14 0x566f80af in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4959
#15 0x566f86aa in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#16 0x566dc8bc in vm_run_global /root/jerryscript/jerry-core/vm/vm.c:350
#17 0x565f388a in jerry_run /root/jerryscript/jerry-core/api/jerry.c:608
#18 0x565ec609 in main /root/jerryscript/jerry-main/main-unix.c:123
#19 0xf7722f20 in __libc_start_main (/lib32/libc.so.6+0x18f20)
#20 0x565eb000 (/root/jerryscript/build/bin/jerry+0x1000)
```

0xf5b00925 is located 0 bytes to the right of 21-byte region [0xf5b00910,0xf5b00925) allocated by thread T0 here:

```
#0 0xf7a93f54 in malloc (/usr/lib32/libasan.so.4+0xe5f54)
#1 0x56695fd4 in jmem_heap_alloc /root/jerryscript/jerry-core/jmem/jmem-heap.c:254
#2 0x566960ce in jmem_heap_gc_and_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:291
#3 0x56696161 in jmem_heap_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:325
#4 0x566f890c in ecma_alloc_string_buffer /root/jerryscript/jerry-core/ecma/base/ecma-alloc.c:222
#5 0x56615741 in ecma_new_ecma_string_from_utf8_buffer /root/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:263
#6 0x56615741 in ecma_new_ecma_string_from_utf8 /root/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:357
#7 0x5662cf0b in ecma_find_or_create_literal_string /root/jerryscript/jerry-core/ecma/base/ecma-literal-storage.c:170
#8 0x566a314a in parser_post_processing /root/jerryscript/jerry-core/parser/js/js-parser.c:1312
#9 0x566a7726 in parser_parse_source /root/jerryscript/jerry-core/parser/js/js-parser.c:2019
#10 0x566abd30 in parser_parse_script /root/jerryscript/jerry-core/parser/js/js-parser.c:2806
#11 0x565f340b in jerry_parse /root/jerryscript/jerry-core/api/jerry.c:459
#12 0x565ec536 in main /root/jerryscript/jerry-main/main-unix.c:112
#13 0xf7722f20 in __libc_start_main (/lib32/libc.so.6+0x18f20)
```

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/jerryscript/jerry-core/parser/js/js-lexer.c:1396 in lexer_parse_number
Shadow bytes around the buggy address:

```
0x3eb600d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3eb600e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3eb600f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3eb60100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3eb60110: fa fa fa fa fa 00 00 00 fa fa 00 00 00 fa
=>0x3eb60120: fa 00 00[05]fa fa fd fd fd fa fa 00 00
0x3eb60130: 00 fa fa fa 00 00 00 fa fa 00 00 04 fa fa fa
0x3eb60140: 00 00 00 00 fa fa 00 00 05 fa fa 00 00 00 fa
0x3eb60150: fa fa 00 00 00 fa fa 00 00 00 00 fa fa 00 00
0x3eb60160: 00 fa fa fa 00 00 00 00 fa 00 00 00 00 fa fa
0x3eb60170: 00 00 00 00 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
==15467==ABORTING
```

Credits: Found by chong from OWL337.

 **rerobika** added a commit to rerobika/jerryscript that referenced this issue on Jan 11, 2021

 Fix underscore lookahead in hex literal parsing ...

a2a1c97

 **rerobika** mentioned this issue on Jan 11, 2021

Fix underscore lookahead in hex literal parsing #4448

 Merged

 **rerobika** self-assigned this on Jan 11, 2021

 **rerobika** added the **bug** label on Jan 11, 2021

 **dbatyai** closed this as completed in [#4448](#) on Jan 11, 2021

 **dbatyai** pushed a commit that referenced this issue on Jan 11, 2021

 Fix underscore lookahead in hex literal parsing ([#4448](#)) ...

✓ 5cef002

Assignees

 **rerobika**

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix underscore lookahead in hex literal parsing**
rerobika/jerryscript

2 participants