New issue

Jump to bottom

heap-use-after-free in the ecma_ref_ecma_string #3748

Closed   **owl337** opened this issue on May 16, 2020 · 0 comments · Fixed by #3765

Assignees

owl337 commented on May 16, 2020 • edited

JerryScript revision

`bd1c4df`

Build platform

Ubuntu 16.04.6 LTS (Linux 4.15.0-99-generic x86_64)

Build steps

```
python ./tools/build.py --clean --debug --compile-flag=-fsanitize=address --compile-flag=-m32 --compile-flag=-fno-omit-frame-pointer --compile-flag=-fno-common --lto=off --error-message=on --system-allocator=on
```

Test case

```
var o = []

function add(i)
{
delete o[i & 31];
new RegExp([
'"\u',
], "g").exec(1);
}

for (var i = 0; i < 130; i++)
{
add(i)
}
```

Output

```
==================================================================
==97694==ERROR: AddressSanitizer: heap-use-after-free on address 0xf61005b0 at pc 0x080605b2 bp 0xff856d28 sp 0xff856d18
READ of size 4 at 0xf61005b0 thread T0
#0 0x80605b1 in ecma_ref_ecma_string /home/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:772
#1 0x808ef54 in ecma_regexp_create_props /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:144
#2 0x808f562 in ecma_op_regexp_initialize /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:322
#3 0x808f850 in ecma_op_create_regexp_from_pattern /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:393
#4 0x80dd0ed in ecma_builtin_regexp_dispatch_helper /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:179
#5 0x80dd154 in ecma_builtin_regexp_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:223
#6 0x807ae83 in ecma_builtin_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1160
#7 0x8084a81 in ecma_op_function_construct /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1229
#8 0x80b7b62 in opfunc_construct /home/jerryscript/jerry-core/vm/vm.c:849
#9 0x80c2df8 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4151
#10 0x80c32fb in vm_run /home/jerryscript/jerry-core/vm/vm.c:4232
#11 0x8083ff1 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:886
#12 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#13 0x80b75f1 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:764
#14 0x80c2de5 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4130
#15 0x80c32fb in vm_run /home/jerryscript/jerry-core/vm/vm.c:4232
#16 0x80b6f6a in vm_run_global /home/jerryscript/jerry-core/vm/vm.c:321
#17 0x804e249 in jerry_run /home/jerryscript/jerry-core/api/jerry.c:596
#18 0x804ad3f in main /home/jerryscript/jerry-main/main-unix.c:759
#19 0xf7875636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
#20 0x8049030 (/home/jerryscript/build/bin/jerry+0x8049030)
```

```
0xf61005b0 is located 0 bytes inside of 15-byte region [0xf61005b0,0xf61005bf)
freed by thread T0 here:
#0 0xf7aa9a84 in free (/usr/lib32/libasan.so.2+0x96a84)
#1 0x8095b14 in jmem_heap_free_block_internal /home/jerryscript/jerry-core/jmem/jmem-heap.c:476
#2 0x8095eac in jmem_heap_free_block /home/jerryscript/jerry-core/jmem/jmem-heap.c:685
#3 0x80c3453 in ecma_dealloc_string_buffer /home/jerryscript/jerry-core/ecma/base/ecma-alloc.c:208
#4 0x806096f in ecma_destroy_ecma_string /home/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:844
#5 0x8060740 in ecma_deref_ecma_string /home/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:816
#6 0x808f7e1 in ecma_op_create_regexp_from_pattern /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:384
#7 0x80dd0ed in ecma_builtin_regexp_dispatch_helper /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:179
#8 0x80dd154 in ecma_builtin_regexp_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:223
#9 0x807ae83 in ecma_builtin_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1160
#10 0x8084a81 in ecma_op_function_construct /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1229
#11 0x80b7b62 in opfunc_construct /home/jerryscript/jerry-core/vm/vm.c:849
#12 0x80c2df8 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4151
#13 0x80c32fb in vm_run /home/jerryscript/jerry-core/vm/vm.c:4232
#14 0x8083ff1 in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:886
#15 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#16 0x80b75f1 in opfunc_call /home/jerryscript/jerry-core/vm/vm.c:764
#17 0x80c2de5 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4130
#18 0x80c32fb in vm_run /home/jerryscript/jerry-core/vm/vm.c:4232
#19 0x80b6f6a in vm_run_global /home/jerryscript/jerry-core/vm/vm.c:321
#20 0x804e249 in jerry_run /home/jerryscript/jerry-core/api/jerry.c:596
#21 0x804ad3f in main /home/jerryscript/jerry-main/main-unix.c:759
#22 0xf7875636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)

previously allocated by thread T0 here:
#0 0xf7aa9dee in malloc (/usr/lib32/libasan.so.2+0x96dee)
#1 0x809581b in jmem_heap_alloc /home/jerryscript/jerry-core/jmem/jmem-heap.c:254
#2 0x80958eb in jmem_heap_gc_and_alloc_block /home/jerryscript/jerry-core/jmem/jmem-heap.c:289
#3 0x809596a in jmem_heap_alloc_block /home/jerryscript/jerry-core/jmem/jmem-heap.c:323
#4 0x8066032 in ecma_stringbuilder_create_from /home/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:2456
#5 0x80c8f17 in ecma_builtin_array_prototype_join /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:368
#6 0x80cd66a in ecma_builtin_array_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2653
#7 0x807aa06 in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1095
#8 0x807abac in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1119
#9 0x8083dce in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:782
#10 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#11 0x80c885f in ecma_builtin_array_prototype_object_to_string /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:151
#12 0x80cd4d5 in ecma_builtin_array_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2596
#13 0x807aa06 in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1095
#14 0x807abac in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1119
#15 0x8083dce in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:782
#16 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#17 0x80877f8 in ecma_op_general_object_ordinary_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects-general.c:324
#18 0x8087718 in ecma_op_general_object_default_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects-general.c:289
#19 0x808bc85 in ecma_op_object_default_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:1720
#20 0x80803b5 in ecma_op_to_primitive /home/jerryscript/jerry-core/ecma/operations/ecma-conversion.c:199
#21 0x80809c0 in ecma_op_to_string /home/jerryscript/jerry-core/ecma/operations/ecma-conversion.c:413
#22 0x809322a in ecma_regexp_read_pattern_str_helper /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:1618
#23 0x808f694 in ecma_op_create_regexp_from_pattern /home/jerryscript/jerry-core/ecma/operations/ecma-regexp-object.c:352
#24 0x80dd0ed in ecma_builtin_regexp_dispatch_helper /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:179
#25 0x80dd154 in ecma_builtin_regexp_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-regexp.c:223
#26 0x807ae83 in ecma_builtin_dispatch_construct /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1160
#27 0x8084a81 in ecma_op_function_construct /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1229
#28 0x80b7b62 in opfunc_construct /home/jerryscript/jerry-core/vm/vm.c:849
#29 0x80c2df8 in vm_execute /home/jerryscript/jerry-core/vm/vm.c:4151

SUMMARY: AddressSanitizer: heap-use-after-free /home/jerryscript/jerry-core/ecma/base/ecma-helpers-string.c:772 ecma_ref_ecma_string
Shadow bytes around the buggy address:
0x3ec20060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec20070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec20080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec20090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec200a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x3ec200b0: fa fa fa fa fa fa[fd]fd fa fa fd fa fa fa fd fa
0x3ec200c0: fa fa 00 07 fa fa 00 05 fa fa 00 07 fa fa fd fd
0x3ec200d0: fa fa 00 00 fa fa 00 05 fa fa 00 05 fa fa 00 07
0x3ec200e0: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fd
0x3ec200f0: fa fa 00 00 fa fa 00 00 fa fa 00 06 fa fa 00 00
0x3ec20100: 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
==97694==ABORTING
```

Credits: This vulnerability is detected by chong from OWL337.

galpeter self-assigned this on May 18, 2020

galpeter mentioned this issue on May 19, 2020

Fix releasing the pattern string in regexp #3765

Merged

dbatyai closed this as completed in #3765 on May 20, 2020

Assignees

galpeter

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix releasing the pattern string in regexp
galpeter/jerryscript

2 participants