heap-buffer-overflow in the jmem_pools_collect_empty #3749

Closed **owl337** opened this issue on May 17, 2020 · 0 comments · Fixed by #3765

Assignees

owl337 commented on May 17, 2020

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

```
try {
[].length = {
valueOf: function() {
return String("abcdabcd").split("").push (-62167219200000,
'"\ubad"',
'"\u', new RegExp([
4294967294,
], "g").exec(1), 1, 1, 1, 1, 1, 1), Object.freeze (Array.prototype);
}
}
assert (false);
}
catch (e) {
Array.prototype.splice(Function.prototype, ("function a() { return 8; }"), this);
}
```

Output

Script Error: TypeError: Invalid argument type.

```
==97903==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xf6000260 at pc 0x0809632c bp 0xfff4f018 sp 0xfff4f008
READ of size 4 at 0xf6000260 thread T0
#0 0x809632b in jmem_pools_collect_empty /home/jerryscript/jerry-core/jmem/jmem-poolman.c:165
#1 0x8095f01 in jmem_pools_finalize /home/jerryscript/jerry-core/jmem/jmem-poolman.c:44
#2 0x809553f in jmem_finalize /home/jerryscript/jerry-core/jmem/jmem-allocator.c:161
#3 0x804d6a6 in jerry_cleanup /home/jerryscript/jerry-core/api/jerry.c:255
#4 0x804b545 in main /home/jerryscript/jerry-main/main-unix.c:994
#5 0xf7801636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
#6 0x8049030 (/home/jerryscript/build/bin/jerry+0x8049030)
```

```
0xf6000260 is located 8 bytes to the right of 8-byte region [0xf6000250,0xf6000258)
allocated by thread T0 here:
#0 0xf7a35dee 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 0x8095952 in jmem_heap_alloc_block_internal /home/jerryscript/jerry-core/jmem/jmem-heap.c:308
#4 0x809606b in jmem_pools_alloc /home/jerryscript/jerry-core/jmem/jmem-poolman.c:85
#5 0x80c3351 in ecma_alloc_number /home/jerryscript/jerry-core/ecma/base/ecma-alloc.c:57
#6 0x806737c in ecma_create_float_number /home/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c:487
#7 0x8067fc4 in ecma_copy_value /home/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c:838
#8 0x8068172 in ecma_fast_copy_value /home/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c:881
#9 0x8089f60 in ecma_op_object_find_own /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:505
#10 0x808a810 in ecma_op_object_get_with_receiver /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:830
#11 0x808a916 in ecma_op_object_get /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:799
#12 0x808a916 in ecma_op_object_get_by_uint32_index /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:862
#13 0x80c8d98 in ecma_op_array_get_to_string_at_index /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:310
#14 0x80c8ed9 in ecma_builtin_array_prototype_join /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:360
#15 0x80cd66a in ecma_builtin_array_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2653
#16 0x807aa06 in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1095
#17 0x807abac in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1119
#18 0x8083dce in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:782
#19 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#20 0x80c885f in ecma_builtin_array_prototype_object_to_string /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:151
#21 0x80cd4d5 in ecma_builtin_array_prototype_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2596
#22 0x807aa06 in ecma_builtin_dispatch_routine /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1095
#23 0x807abac in ecma_builtin_dispatch_call /home/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1119
#24 0x8083dce in ecma_op_function_call_simple /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:782
#25 0x8084716 in ecma_op_function_call /home/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1085
#26 0x80877f8 in ecma_op_general_object_ordinary_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects-general.c:324
#27 0x8087718 in ecma_op_general_object_default_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects-general.c:289
#28 0x808bc85 in ecma_op_object_default_value /home/jerryscript/jerry-core/ecma/operations/ecma-objects.c:1720
#29 0x80803b5 in ecma_op_to_primitive /home/jerryscript/jerry-core/ecma/operations/ecma-conversion.c:199
#30 0x80809c0 in ecma_op_to_string /home/jerryscript/jerry-core/ecma/operations/ecma-conversion.c:413

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jerryscript/jerry-core/jmem/jmem-poolman.c:165 jmem_pools_collect_empty
Shadow bytes around the buggy address:
0x3ebffff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x3ec00000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec00010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec00020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ec00030: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
=>0x3ec00040: fa fa fd fa fa fa fd fa fa fa 00 fa[fa]fa fd fa
0x3ec00050: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x3ec00060: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
0x3ec00070: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fa
0x3ec00080: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fa
0x3ec00090: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fd
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
==97903==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