

New issue

Jump to bottom

# heap-use-after-free in ecma\_is\_lexical\_environment #4445

Closed owl337 opened this issue on Jan 11, 2021 · 0 comments · Fixed by #4458

Assignees



Labels

bug

owl337 commented on Jan 11, 2021

JerryScript revision

fdaacde

Build platform

Ubuntu 16.04.6 LTS (Linux 4.4.0-179-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-ld=gold \
--error-messages=on --profile=es2015-subset
```

Test case

```
var a = ["", "\0", "\t", "\n", "\v", "\f", "\r", " ", "\u00a0", "\u2028", "\u2029", "\uffeff"]
Array.prototype[4] = 10;
function Test()
{
    a.sort(function() {
        var A = function() { };
        A.prototype.x = 42;
        var o = new Proxy({
            "3": {
                writable:false,
                value:20
            }
        }, {
            getPrototypeOf: function (val, size, ch) {
                var result = new String(val);
                if (ch == null) {
                    ch = "";
                }
                while (result.length < size) {
                    result = ch + result;
                }
                return result;
            }
        });
    o.x = 43;
    var result = "";
    for (var p in o)
        result += o[p];
    return a | 0;
});
WScript.Echo(a);
Test();
```

Execution steps

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

Output

```
=====
==179417==ERROR: AddressSanitizer: heap-use-after-free on address 0xf5304720 at pc 0x566b5311 bp 0xff9aa468 sp 0xff9aa458
READ of size 2 at 0xf5304720 thread T0
#0 0x566b5310 in ecma_is_lexical_environment /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:177
#1 0x566b5447 in ecma_get_object_type /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:203
#2 0x56670759 in ecma_op_object_get_own_property_descriptor /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:1862
#3 0x56672f01 in ecma_op_object_enumerate /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:2513
#4 0x56612f78 in opfunc_for_in /root/jerryscript/jerry-core/vm/opcodes.c:368
#5 0x56630ffe in vm_loop_lto_priv_465 /root/jerryscript/jerry-core/vm/vm.c:3986
#6 0x565f87c3 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4953
#7 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#8 0x566a74be in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1182
#9 0x566a8106 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1412
#10 0x565fc0b9 in ecma_builtin_array_prototype_object_sort_compare_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1063
#11 0x565ddfaa in ecma_builtin_helper_array_merge_sort_bottom_up /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:47
#12 0x565de1f0 in ecma_builtin_helper_array_merge_sort_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:109
#13 0x565fc84f in ecma_builtin_array_prototype_object_sort /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1184
#14 0x566030f9 in ecma_builtin_array_prototype_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2918
```

```
#15 0x566cf1d0 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1490
#16 0x566cf466 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1522
#17 0x566a7805 in ecma_op_function_call_native /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1246
#18 0x566a8125 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1416
#19 0x5661dd7d in opfunc_call_lto_priv.464 /root/jerryscript/jerry-core/vm/vm.c:822
#20 0x565f8827 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4959
#21 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#22 0x566a74be in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1182
#23 0x566a8106 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1412
#24 0x5661dd7d in opfunc_call_lto_priv.464 /root/jerryscript/jerry-core/vm/vm.c:822
#25 0x565f8827 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4959
#26 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#27 0x5661c015 in vm_run_global /root/jerryscript/jerry-core/vm/vm.c:350
#28 0x566e3344 in jerry_run /root/jerryscript/jerry-core/api/jerry.c:608
#29 0x566dc51a in main /root/jerryscript/jerry-main/main-unix.c:123
#30 0xf6f11f20 in __libc_start_main (/lib32/libc.so.6+0x18f20)
#31 0x565877e0 (/root/jerryscript/build3/bin/jerry+0x1d7e0)
```

0xf5304720 is located 0 bytes inside of 24-byte region [0xf5304720,0xf5304738)

freed by thread T0 here:

```
#0 0xf72a0b94 in __interceptor_free (/usr/lib32/libasan.so.4+0xe5b94)
#1 0x566384f0 in jmem_heap_free_block_internal /root/jerryscript/jerry-core/jmem/jmem-heap.c:478
#2 0x566388b9 in jmem_heap_free_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:692
#3 0x565f8ed9 in ecma_dealloc_extended_object /root/jerryscript/jerry-core/ecma/base/ecma-alloc.c:123
#4 0x566f6c53 in ecma_gc_free_object /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:1763
#5 0x566f78c6 in ecma_gc_run /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:1891
#6 0x566f7aa6 in ecma_free_unused_memory /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:1935
#7 0x56638278 in jmem_heap_gc_and_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:285
#8 0x56638318 in jmem_heap_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:325
#9 0x56671b58 in ecma_object_sort_property_names /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:2262
#10 0x56672c78 in ecma_op_object_own_property_keys /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:2463
#11 0x56672dba in ecma_op_object_enumerate /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:2489
#12 0x56612f78 in opfunc_for_in /root/jerryscript/jerry-core/vm/opcodes.c:368
#13 0x56630ffe in vm_loop_lto_priv.465 /root/jerryscript/jerry-core/vm/vm.c:3986
#14 0x565f87c3 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4953
#15 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#16 0x566a74be in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1182
#17 0x566a8106 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1412
#18 0x565fc0b9 in ecma_builtin_array_prototype_object_sort_compare_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1063
#19 0x565d0fba in ecma_builtin_helper_array_merge_sort_bottom_up /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:47
#20 0x565de1f0 in ecma_builtin_helper_array_merge_sort_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:109
#21 0x565fc84f in ecma_builtin_array_prototype_object_sort /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1184
#22 0x566030f9 in ecma_builtin_array_prototype_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2918
#23 0x566cf1d0 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1490
#24 0x566cf466 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1522
#25 0x566a7805 in ecma_op_function_call_native /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1246
#26 0x566a8125 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1416
#27 0x5661dd7d in opfunc_call_lto_priv.464 /root/jerryscript/jerry-core/vm/vm.c:822
#28 0x565f8827 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4959
#29 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
```

previously allocated by thread T0 here:

```
#0 0xf72a0f54 in malloc (/usr/lib32/libasan.so.4+0xe5f54)
#1 0x566381a8 in jmem_heap_alloc /root/jerryscript/jerry-core/jmem/jmem-heap.c:254
#2 0x56638286 in jmem_heap_gc_and_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:291
#3 0x56638318 in jmem_heap_alloc_block /root/jerryscript/jerry-core/jmem/jmem-heap.c:325
#4 0x565f8eb6 in ecma_alloc_extended_object /root/jerryscript/jerry-core/ecma/base/ecma-alloc.c:109
#5 0x5664d4fa in ecma_create_object /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:82
#6 0x5668ae26 in ecma_op_create_string_object /root/jerryscript/jerry-core/ecma/operations/ecma-string-object.c:83
#7 0x565f76f7 in ecma_builtin_string_dispatch_construct /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-string.c:387
#8 0x566cf78a in ecma_builtin_dispatch_construct /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1555
#9 0x566a8631 in ecma_op_function_construct /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1562
#10 0x5661e2f4 in opfunc_construct_lto_priv.461 /root/jerryscript/jerry-core/vm/vm.c:907
#11 0x565f8805 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4980
#12 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#13 0x566a74be in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1182
#14 0x566a8106 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1412
#15 0x56678cd3 in ecma_proxy_object_get_prototype_of /root/jerryscript/jerry-core/ecma/operations/ecma-proxy-object.c:318
#16 0x56673108 in ecma_op_object_enumerate /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c:2552
#17 0x56612f78 in opfunc_for_in /root/jerryscript/jerry-core/vm/opcodes.c:368
#18 0x56630ffe in vm_loop_lto_priv.465 /root/jerryscript/jerry-core/vm/vm.c:3986
#19 0x565f87c3 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:4953
#20 0x565f8e0c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5060
#21 0x566a74be in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1182
#22 0x566a8106 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-function-object.c:1412
#23 0x565fc0b9 in ecma_builtin_array_prototype_object_sort_compare_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1063
#24 0x565d0fba in ecma_builtin_helper_array_merge_sort_bottom_up /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:47
#25 0x565de1f0 in ecma_builtin_helper_array_merge_sort_helper /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-helpers-sort.c:109
#26 0x565fc84f in ecma_builtin_array_prototype_object_sort /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:1184
#27 0x566030f9 in ecma_builtin_array_prototype_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtin-array-prototype.c:2918
#28 0x566cf1d0 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1490
#29 0x566cf466 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ecma-builtins.c:1522
```

SUMMARY: AddressSanitizer: heap-use-after-free /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:177 in ecma\_is\_lexical\_environment

Shadow bytes around the buggy address:

```
0x3ea60890: fd fd fd fa fa fd fd fd fa fa fd fd fd fa
0x3ea608a0: fa fa fd fd fd fa fa fd fd fd fa fa fd fd
0x3ea608b0: fd fa fa fd fd fd fa fa fa fa fa fa fa fa
0x3ea608c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3ea608d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
->0x3ea608e0: fa fa fa fa[fd]fd fd fa fa fd fd fd fa fa
0x3ea608f0: fd fd fd fa fa fd fd fd fa fa 00 00 00 fa
0x3ea60900: fa fa 00 00 00 fa fa 00 00 00 fa fa 00 00
0x3ea60910: 00 fa fa 00 00 00 fa fa 00 00 00 fa fa
0x3ea60920: 00 00 00 fa fa 00 00 00 fa fa fd fd fd fd
0x3ea60930: fa fa fd fd fd fa fa fd 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
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
==179417==ABORTING
```

Credits: Found by chong from OWL337.


 rerobika assigned galpeter on Jan 11, 2021

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

 galpeter mentioned this issue on Jan 13, 2021

Fix prototype chain traversing #4458

 Merged

 dbatyai closed this as completed in #4458 on Jan 15, 2021

#### Assignees

 galpeter

#### Labels

`bug`

#### Projects


None yet

#### Milestone

No milestone

#### Development

Successfully merging a pull request may close this issue.

 Fix prototype chain traversing  
galpeter/jerryscript

#### 3 participants

