

New issue

[Jump to bottom](#)

SEGV in ecma_ref_object_inline of ecma-gc.c #4871

🔒 Closed

hope-fly opened this issue on Dec 9, 2021 · 0 comments · Fixed by [#4885](#)

Assignees



Labels

bug

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 echo(str) {
  console.log(str);
}

function T(p, r, u) {
  return Object.assign(p, {
    then(onFulfilled, onRejected) {
      if (u) {
        onFulfilled(r);
      } else {
        onFulfilled();
      }
    }
  });
}
```

```

        return Promise.prototype.then.call(this, onFulfilled, onRejected);
    }
});
}

function JSEtest(i) {
    var ps = [T(Promise.resolve('success'))];
    Promise.all(ps).then(res => {
        echo(`Test #${i} - Success with '${res}' (length = ${res.length}) (isArray = ${Array.isArray(res)})`);
    }).catch(err => {
        echo(`Test #${i} - Catch with ${err}`);
    });
}

JSEtest(1);

```



Execution steps & Output

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

```
ASAN:DEADLYSIGNAL
```

```
=====
```

```
==95503==ERROR: AddressSanitizer: SEGV on unknown address 0x41b58ab0 (pc 0x566075cf bp 0x1ff7c4b0 sp
==95503==The signal is caused by a READ memory access.
```

```

#0 0x566075ce in ecma_ref_object_inline /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:136
#1 0x56639c0c in ecma_copy_value /root/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c:913
#2 0x56639c0c in ecma_fast_copy_value /root/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c
#3 0x566cdd0b in ecma_op_object_find_own /root/jerryscript/jerry-core/ecma/operations/ecma-object
#4 0x566d2ea0 in ecma_op_object_find_own /root/jerryscript/jerry-core/ecma/operations/ecma-object
#5 0x566d2ea0 in ecma_op_object_get_with_receiver /root/jerryscript/jerry-core/ecma/operations/ec
#6 0x567ef0cf in ecma_op_array_get_to_string_at_index /root/jerryscript/jerry-core/ecma/builtin-o
#7 0x567ef0cf in ecma_builtin_array_prototype_join /root/jerryscript/jerry-core/ecma/builtin-obje
#8 0x567ef0cf in ecma_builtin_array_prototype_dispatch_routine /root/jerryscript/jerry-core/ecma/
#9 0x566731f1 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects/
#10 0x566731f1 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ec
#11 0x566b48b4 in ecma_op_function_call_native_built_in /root/jerryscript/jerry-core/ecma/operati
#12 0x566bae4d in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-functio
#13 0x5668d365 in ecma_array_object_to_string /root/jerryscript/jerry-core/ecma/operations/ecma-a
#14 0x5681e945 in ecma_builtin_intrinsic_dispatch_routine /root/jerryscript/jerry-core/ecma/built
#15 0x566731f1 in ecma_builtin_dispatch_routine /root/jerryscript/jerry-core/ecma/builtin-objects
#16 0x566731f1 in ecma_builtin_dispatch_call /root/jerryscript/jerry-core/ecma/builtin-objects/ec
#17 0x566b48b4 in ecma_op_function_call_native_built_in /root/jerryscript/jerry-core/ecma/operati
#18 0x566bae4d in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-functio
#19 0x566c9572 in ecma_op_general_object_ordinary_value /root/jerryscript/jerry-core/ecma/operati
#20 0x566c976b in ecma_op_general_object_default_value /root/jerryscript/jerry-core/ecma/operatio
#21 0x566d6875 in ecma_op_object_default_value /root/jerryscript/jerry-core/ecma/operations/ecma-
#22 0x566a905a in ecma_op_to_string /root/jerryscript/jerry-core/ecma/operations/ecma-conversion.
#23 0x567b3433 in vm_loop /root/jerryscript/jerry-core/vm/vm.c:2820
#24 0x567e21da in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5260

```

```
#25 0x567e7e7c in vm_run /root/jerryscript/jerry-core/vm/vm.c:5363
#26 0x566b4101 in ecma_op_function_call_simple /root/jerryscript/jerry-core/ecma/operations/ecma-
#27 0x566bae25 in ecma_op_function_call /root/jerryscript/jerry-core/ecma/operations/ecma-functio
#28 0x566c495e in ecma_process_promise_reaction_job /root/jerryscript/jerry-core/ecma/operations/
#29 0x566c495e in ecma_process_all_enqueued_jobs /root/jerryscript/jerry-core/ecma/operations/ecm
#30 0x565d4dbc in jerry_run_jobs /root/jerryscript/jerry-core/api/jerryscript.c:1064
#31 0x565c004b in main /root/jerryscript/jerry-main/main-jerry.c:326
#32 0xf76f1f20 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18f20)
#33 0x565c9359 (/root/jerryscript/build/bin/jerry+0x3b359)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:136 in ecma_ref_obje
==95503==ABORTING



Credits: Found by OWL337 team.

  rerobika added the **bug** label on Dec 9, 2021

  rerobika self-assigned this on Dec 9, 2021

 rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 9, 2021

 Fix invalid argument reference in Promise.all executor ...

✓ bf96d98

  rerobika mentioned this issue on Dec 9, 2021

Fix invalid argument reference in Promise.all executor #4885

 Merged

  hope-fly mentioned this issue on Dec 13, 2021

**Assertion 'ecma_is_lexical_environment (object_p)' failed at ecma-helpers.c
(ecma_get_lex_env_type). #4902**

 Closed

 ossy-szeged closed this as completed in [#4885](#) on Dec 15, 2021

 ossy-szeged pushed a commit that referenced this issue on Dec 15, 2021





Fix invalid argument reference in Promise.all executor ([#4885](#)) ...

✓ ee59c22

Assignees

 rerobika

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix invalid argument reference in Promise.all executor**
rerobika/jerryscript

2 participants

