jerryscript-project / **jerryscript** Public

Code · Issues 71 · Pull requests 39 · Actions · Wiki · Security · •••

New issue

Jump to bottom

Stack-overflow in ecma-objects (ecma_op_object_find_own) #4848

Closed **hope-fly** opened this issue on Dec 7, 2021 · 1 comment · Fixed by #4877

Labels bug stack-overflow

hope-fly commented on Dec 7, 2021 • edited

JerryScript revision

4592143

Build platform

Ubuntu 18.04.5 LTS (Linux 4.19.128-microsoft-standard x86_64)
Ubuntu 18.04.5 LTS (Linux 5.4.0-44-generic x86_64)

Build steps

```
./tools/build.py --clean --debug --compile-flag=-fsanitize=address --compile-flag=-m32 --lto=off --lo
```

Test case

```
var once = false;
var m = 1;

function JSEtest(){
  if(!once){
    m = new Array(1, 2, 3);
    this[2] = m;
  }
  once = true;
  return this[2] = m;
}
```

```
JSON.parse("[1, 2, [4, 5]]", JSEtest);
```

Execution steps & Output

```
$ ./jerryscript/build/bin/jerry poc1.js

ASAN:DEADLYSIGNAL
=================================================================
==5376==ERROR: AddressSanitizer: stack-overflow on address 0xff3e5ff0 (pc 0x56722cec bp 0x00000000 sp
    #0 0x56722ceb in ecma_op_object_find_own /root/jerryscript/jerry-core/ecma/operations/ecma-object
    #1 0x56a4ae1f  (/root/jerryscript/build/bin/jerry+0x46fe1f)

SUMMARY: AddressSanitizer: stack-overflow /root/jerryscript/jerry-core/ecma/operations/ecma-objects.c
==5376==ABORTING
```

Credits: Found by OWL337 team.

rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 7, 2021

`Prevent arguments object creation if arguments parameter is present` … ✓ `0be4870`

rerobika mentioned this issue on Dec 7, 2021

Prevent arguments object creation if 'arguments' function argument is present #4849

Merged

rerobika added bug stack-overflow labels on Dec 8, 2021

rerobika commented on Dec 8, 2021 Member

Thanks for the report, that's a real stack-overflow issue.

👍 1

eternalsakura mentioned this issue on Dec 8, 2021

AddressSanitizer: heap-use-after-free jerry-core/ecma/base/ecma-gc.c:90 in ecma_gc_set_object_visited #4870

Open

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

`Prevent stackoverflow in json internalize property` … ✓ 33c0dfa

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

`Prevent stack-overflow in json internalize property` … ✓ d040dc4

This was referenced on Dec 9, 2021

Prevent stack-overflow in json internalize property #4877

Merged

AddressSanitizer: stack-overflow in ecma_builtin_json_internalize_process_property #4883

Closed

rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 15, 2021

`Prevent stack-overflow in json internalize property` … ✓ 73ab9ee

ossy-szeged closed this as completed in #4877 on Dec 15, 2021

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

`Prevent stack-overflow in json internalize property (#4877)` … ✓ dfc001d

Assignees

No one assigned

Labels

bug stack-overflow

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Prevent stack-overflow in json internalize property
rerobika/jerryscript

2 participants