

New issue

[Jump to bottom](#)

## Stack-overflow in vm\_loop.lto\_priv.304 of vm.c #4901

🔒 Closed

hope-fly opened this issue on Dec 13, 2021 · 0 comments · Fixed by [#4945](#)

Assignees



Labels

stack-overflow

hope-fly commented on Dec 13, 2021 • edited ▼

JerryScript revision

Commit: [42523bd6](#)

Version: v3.0.0

Build platform

Ubuntu 18.04.5 LTS (Linux 5.4.0-44-generic x86\_64)

Build steps

```
python ./tools/build.py --clean --debug --compile-flag=-fsanitize=address --compile-flag=-m32 --comp
```

Test case

```
function JSEtest() {  
  new JSEtest();  
}  
  
try {  
  JSEtest();  
} catch (e) {  
  print(e);  
}
```

## Execution steps & Output

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

ASAN:DEADLYSIGNAL

```
=====
==78723==ERROR: AddressSanitizer: stack-overflow on address 0xff0d8f90 (pc 0x566a456c bp 0xff0d95d8 s
#0 0x566a456b in vm_loop.lto_priv.304 /root/jerryscript/jerry-core/vm/vm.c:975
#1 0x56929645 in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5260
#2 0x5692e592 in vm_run /root/jerryscript/jerry-core/vm/vm.c:5363
#3 0x5674524e in ecma_op_function_call_simple.lto_priv.397 /root/jerryscript/jerry-core/ecma/oper
#4 0x567e8c9c in ecma_op_function_construct_simple /root/jerryscript/jerry-core/ecma/operations/e
#5 0x567e8c9c in ecma_op_function_construct /root/jerryscript/jerry-core/ecma/operations/ecma-fun
#6 0x5692995a in opfunc_construct.isra.2 /root/jerryscript/jerry-core/vm/vm.c:844
#7 0x5692995a in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5287
#.....

#.....
#368 0x5692e592 in vm_run /root/jerryscript/jerry-core/vm/vm.c:5363
#369 0x5674524e in ecma_op_function_call_simple.lto_priv.397 /root/jerryscript/jerry-core/ecma/op
#370 0x567e8c9c in ecma_op_function_construct_simple /root/jerryscript/jerry-core/ecma/operations
#371 0x567e8c9c in ecma_op_function_construct /root/jerryscript/jerry-core/ecma/operations/ecma-f
#372 0x5692995a in opfunc_construct.isra.2 /root/jerryscript/jerry-core/vm/vm.c:844
#373 0x5692995a in vm_execute /root/jerryscript/jerry-core/vm/vm.c:5287
```

```
SUMMARY: AddressSanitizer: stack-overflow /root/jerryscript/jerry-core/vm/vm.c:975 in vm_loop.lto_pri
==78723==ABORTING
```



Credits: Found by OWL337 team.

 **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Dec 22, 2021

 Add stack-overflow check for 'ecma\_op\_function\_call\_simple' ...  60f31d9

 **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Dec 22, 2021

 Add stack-overflow check for 'ecma\_op\_function\_call\_simple' ...  1ad4d87

  **rerobika** assigned **mnegyokru** on Jan 4

  **rerobika** added the `stack-overflow` label on Jan 4

 **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 4

 Add stack-overflow check for general `[[Construct]]` method of function... ... ✓ fca661c

 **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 4

 Add stack-overflow check for general `[[Construct]]` method of function... ... ✓ b4eecfc

  **mnegyokru** mentioned this issue on Jan 4

**Add stack-overflow check for general `[[Construct]]` method of function objects #4945**

 Merged

 **dbatyai** closed this as completed in [#4945](#) on Jan 10

---

 **dbatyai** pushed a commit that referenced this issue on Jan 10

 Add stack-overflow check for general `[[Construct]]` method of function... ... ✓ 58e504f

#### Assignees

 mnegyokru

#### Labels

stack-overflow

#### Projects


None yet

#### Milestone

No milestone

#### Development

Successfully merging a pull request may close this issue.

 **Add stack-overflow check for general `[[Construct]]` method of function objects**  
mnegyokru/jerryscript

---

3 participants

