

New issue

Jump to bottom

# SEGV in ecma\_deref\_ecma\_string #3858

Closed ArrayZWang opened this issue on Jun 4, 2020 · 0 comments · Fixed by #3867

Labels bug ecma core

ArrayZWang commented on Jun 4, 2020 • edited

```
JerryScript revision
c09c2c5

Build platform
Ubuntu 18.04 LTS

Build steps
python tools/build.py --profile=es2015-subset --lto=off --error-messages=on --strip=off --compile-flag=-fsanitize=address

Test case

function main() {
  const v1 = ~2147483649;
  const v3 = v1 / v1;
  const v4 = v3 % "species";
  function v5(v6,v7,v8,v9) {
    const v11 = [1337,1337];
    return v5;
  }
  const v14 = "species".__proto__;
  "species"[4294967297] = v14;
  let v17 = 0;
  while (v17 < 3) {
    const v18 = gc(...v4,3,v4);
  }
  const v19 = "species"[4179111969];
  const v20 = v17 == v4;
  let v21 = 3;
  if (v19) {
    const v23 = {set:v19};
    const v25 = Object.defineProperty("species","constructor",v23);
  } else {
    v21 = 3;
  }
  const v26 = [13.37,13.37];
  const v27 = {toString:0,length:v3,d:0};
  const v28 = v17 - v27;
  const v29 = v19.__proto__;
  const v30 = v19(v4,3,2147483649,v29);
  const v31 = [v21,v29,2147483649,v21];
  const v33 = [1337,1337];
  const v34 = v29 - 1;
  const v35 = [2147483649,13.37,"species"];
  const v36 = {a:13.37,length:13.37};
  const v37 = {constructor:v35};
  let v38 = v33;
  let v41 = 0;
  while (v41 < 1) {
  }
  let v42 = gc;
  v35.__proto__ = v33;
  const v44 = Symbol.iterator;
  const v45 = Symbol[v44];
  const v47 = RegExp(v45);
}
main();


Execution steps
build/bin/jerry testcase.js

Output
AddressSanitizer:DEADLYSIGNAL

Backtrace
Program received signal SIGSEGV, Segmentation fault.
0x0000000004ffd0c in ecma_deref_ecma_string ()
(gdb) bt

#0  0x0000000004ffd0c in ecma_deref_ecma_string ()
#1  0x0000000005a95bb in ofunc_spread_arguments ()
#2  0x000000000560348 in vm_loop ()
#3  0x00000000055b5f6 in vm_execute ()
#4  0x00000000055b193 in vm_run ()
#5  0x00000000051f650 in ecma_op_function_call_simple ()
#6  0x00000000051f2d6 in ecma_op_function_call ()
#7  0x00000000055b9aa in vm_execute ()
#8  0x00000000055b193 in vm_run ()
```

```
#9 0x0000000004f501e in jerry_run ()
#10 0x0000000004f25df in main ().
```

 dbatyai added **bug** **ecma core** labels on Jun 5, 2020

 galpeter mentioned this issue on Jun 5, 2020

**Correct release of spread arguments #3867**

 Merged

 zhczeg closed this as completed in [#3867](#) on Jun 6, 2020

Assignees

No one assigned

Labels

**bug** **ecma core**

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Correct release of spread arguments**  
galpeter/jernyscript

2 participants

