New issue

Jump to bottom

SEGV in jmem_pools_finalize #3859

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

Labels bug ecma builtins

ArayzWang 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 v3 = {a:13.37,length:13.37};
const v6 = [13.37,13.37];
let v9 = 0;
const v10 = v6.copyWithin(v9,8,2147483649);
const v11 = -9007199254740993 == gc;
const v12 = gc(...v11,...v3);
}
main();
```

Execution steps

build/bin/jerry testcase.js

Output

AddressSanitizer:DEADLYSIGNAL

Backtrace

Program received signal SIGSEGV, Segmentation fault.
0x000000000053bd5f in jmem_pools_finalize ()
(gdb) bt

```
#0  0x000000000053bd5f in jmem_pools_finalize ()
#1  0x000000000053a7bb in jmem_finalize ()
#2  0x00000000004f2ba0 in main ()
```

dbatyai assigned szilagyiadam on Jun 5, 2020

dbatyai added bug ecma builtins labels on Jun 5, 2020

galpeter mentioned this issue on Jun 5, 2020

Correct release of spread arguments #3867

Merged

dbatyai unassigned szilagyiadam on Jun 5, 2020

zherczeg closed this as completed in #3867 on Jun 6, 2020

Assignees

No one assigned

Labels

bug ecma builtins

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Correct release of spread arguments
galpeter/jerryscript

3 participants