<> Code ⊙ Issues 71 ⑃ Pull requests 39 ▷ Actions ▥ Wiki ⊘ Security ⋯

New issue

Assertion 'arguments_type != SCANNER_ARGUMENTS_PRESENT && arguments_type != SCANNER_ARGUMENTS_PRESENT_NO_REG' in js-scanner-util (scanner_pop_literal_pool) #4847

⊘ **Closed** **hope-fly** opened this issue on Dec 7, 2021 · 1 comment · Fixed by #4849

Assignees	🐕
Labels	**bug**

---

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 --profile=es2015-subset --compile-flag=-fsanitize=address --
compile-flag=-m32 --lto=off --logging=on --line-info=on --error-message=on --system-allocator=on -
-stack-limit=20
```

Test case

```
this.__defineSetter__("a", function(){});
function JSEtest (arguments = (function rec(n1, n2) {
    if (n1.length == n2) { m = "CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCAAAA"; }
    rec(n1, n2 + 1);
```

```
})([,], 0)
        , m = eval("")
        )
{}
JSEtest(a);
```

Execution steps & Output

```
$ ./jerryscript/build/bin/jerry poc.js
ICE: Assertion 'arguments_type != SCANNER_ARGUMENTS_PRESENT && arguments_type !=
SCANNER_ARGUMENTS_PRESENT_NO_REG' failed at root/jerryscript/jerry-core/parser/js/js-scanner-
util.c(scanner_pop_literal_pool):668.
Error: ERR_FAILED_INTERNAL_ASSERTION
```

Credits: Found by OWL337 team.

🏷 **rerobika** added the **bug** label on Dec 7, 2021

👤 **rerobika** self-assigned this on Dec 7, 2021

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

    🐶 `Prevent arguments object creation if arguments parameter is present` ⋯   ✓ d8d2ec7

🔗 **rerobika** mentioned this issue on Dec 7, 2021

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

(⑂ **Merged**)

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

    🐶 `Prevent arguments object creation if 'arguments' function argument is…` ⋯   ✓ fbb1d4c

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

    🐶 `Prevent arguments object creation if 'arguments' function argument is…` ⋯   ✓ 3bb042b

🟥 **dbatyai** closed this as completed in #4849 on Dec 7, 2021

dbatyai pushed a commit that referenced this issue on Dec 7, 2021

Prevent arguments object creation if 'arguments' function argument is… ... ✓ 18dd9aa

✉ **hope-fly** commented on Dec 7, 2021   Author

Got it！ Thanks for your devotion！
...

Assignees

rerobika

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

ᛦ **Prevent arguments object creation if 'arguments' function argument is present**
rerobika/jerryscript

2 participants