

New issue

Jump to bottom

Assertion '(flags >> CBC\_STACK\_ADJUST\_SHIFT) >= CBC\_STACK\_ADJUST\_BASE || (CBC\_STACK\_ADJUST\_BASE - (flags >> CBC\_STACK\_ADJUST\_SHIFT)) <= context\_p->stack\_depth' in parser\_emit\_cbc\_backward\_branch #3834

Closed owl337 opened this issue on Jun 2, 2020 · 0 comments · Fixed by #3828

Labels bug

owl337 commented on Jun 2, 2020

JerryScript revision

a56e31f

Build platform

Ubuntu 16.04.6 LTS (Linux 4.15.0-99-generic x86\_64)

Build steps

```
./tools/build.py --clean --debug --compile-flag=-fsanitize=address \
--compile-flag=-m32 --compile-flag=-fno-omit-frame-pointer \
--compile-flag=-fno-common --compile-flag=-g \
--strip=off --system-allocator=on --logging=on \
--linker-flag=-fuse-ld=gold --error-messages=on \
--profile=es2015-subset --lto=off --stack-limit=50
```


Test case

```
function dec(x) { return x - 1 };
for (var i = 11; ((123).toString(37)) = dec (i); i--) {}
```

Output

```
ICE: Assertion '(flags >> CBC_STACK_ADJUST_SHIFT) >= CBC_STACK_ADJUST_BASE || (CBC_STACK_ADJUST_BASE - (flags >> CBC_STACK_ADJUST_SHIFT)) <= context_p->stack_depth' failed at
/home/JerryScript/jerry-core/parser/js/js-parser-util.c(parser_emit_cbc_backward_branch):669.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted (core dumped)
```

Credits: This vulnerability is detected by chong from OWL337.

 rerobika linked a pull request on Jun 3, 2020 that will close this issue

Fix assignment lookahead in parser\_process\_group\_expression #3828

Merged

 rerobika added the bug label on Jun 3, 2020

 dbatyai closed this as completed in #3828 on Jun 3, 2020

Assignees

No one assigned

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 Fix assignment lookahead in parser\_process\_group\_expression  
rerobika/jerryscript

2 participants

