New issue

Jump to bottom

Assertion 'context_p->stack_top_uint8 == LEXER_EXPRESSION_START' in parser_parse_expression #3819

Closed **owl337** opened this issue on May 31, 2020 · 0 comments · Fixed by #3828

Assignees

Labels bug

owl337 commented on May 31, 2020 • edited

JerryScript revision

d06c3a7

Build platform

Ubuntu 16.04.6 LTS (Linux 4.15.0-99-generic x86_64)

Build steps

```
python tools/build.py --profile=es2015-subset --lto=off --compile-flag=-g \
--error-messages=on --debug --compile-flag=-g --strip=off --logging=on \
--compile-flag=-fsanitize=address --stack-limit=15
```

Test case

```
typeof (global.v2) = 123;
```

Output

```
ICE: Assertion 'context_p->stack_top_uint8 == LEXER_EXPRESSION_START' failed at /home/JerryScript/jerryscript/jerry-core/parser/js/js-parser-expr.c(parser_parse_expression):3565.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted (core dumped)
```

Credits: This vulnerability is detected by chong from OWL337.

owl337 changed the title ~~ICE: Assertion 'context_p->stack_top_uint8 == LEXER_EXPRESSION_START' failed at /home/JerryScript/jerryscript/jerry-core/parser/js/js-parser-expr.c(parser_parse_expression):3565.~~ Assertion 'context_p->stack_top_uint8 == LEXER_EXPRESSION_START' in parser_parse_expression on May 31, 2020

rerobika self-assigned this on Jun 2, 2020

rerobika added the bug label on Jun 2, 2020

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jun 2, 2020

`Fix assignment lookahead in parser_process_group_expression` ... ✓ b20e100

rerobika linked a pull request on Jun 2, 2020 that will close this issue

Fix assignment lookahead in parser_process_group_expression #3828 Merged

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jun 3, 2020

`Fix assignment lookahead in parser_process_group_expression` ... ✓ f88ec45

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jun 3, 2020

`Fix assignment lookahead in parser_process_group_expression` ... ✓ a7796a1

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jun 3, 2020

`Fix assignment lookahead in parser_process_group_expression` ... ✓ 34c9833

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jun 3, 2020

`Fix assignment lookahead in parser_process_group_expression` ... ✓ b5c2323

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

dbatyai pushed a commit that referenced this issue on Jun 3, 2020

Fix assignment lookahead in parser_process_group_expression (#3828) ··· fe09200

Assignees

rerobika

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