

New issue

Jump to bottom

Assertion 'context\_p->token.type == LEXER\_RIGHT\_BRACE || context\_p->token.type == LEXER\_ASSIGN || context\_p->token.type == LEXER\_COMMA' in parser\_parse\_object\_initializer #3869

Closed owl337 opened this issue on Jun 6, 2020 · 0 comments · Fixed by #3872

Assignees



Labels

bug parser

owl337 commented on Jun 6, 2020

JerryScript revision

cae6cd0

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
```

Test case

```
function a ({
  *;
})
```

Output

```
ICE: Assertion 'context_p->token.type == LEXER_RIGHT_BRACE || context_p->token.type == LEXER_ASSIGN || context_p->token.type == LEXER_COMMA' failed at /home/JerryScript/jerry-core/parser/js/js-parser-expr.c(parser_parse_object_initializer):3234.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted
```

Credits: This vulnerability is detected by chong from OWL337.

zherczeg added a commit to zherczeg/jerryscript that referenced this issue on Jun 8, 2020



Asterisk should be ignored by object initializers. ...

16dc78e

zherczeg mentioned this issue on Jun 8, 2020



Asterisk should be ignored by object initializers. #3872

Merged

rerobika assigned zherczeg on Jun 8, 2020

rerobika added bug parser labels on Jun 8, 2020

rerobika closed this as completed in #3872 on Jun 8, 2020

rerobika pushed a commit that referenced this issue on Jun 8, 2020



Asterisk should be ignored by object initializers. (#3872) ...

✓ 1230d45

Assignees

zherczeg

Labels

bug parser

Projects

None yet

---


Milestone

No milestone

---

Development

Successfully merging a pull request may close this issue.

 **Asterisk should be ignored by object initializers.**  
zhczeg/jerrycript

---

3 participants

