

New issue

Jump to bottom

Assertion 'context.status_flags & PARSER_SCANNING_SUCCESSFUL' in parser_parse_source #3824

Closed owl337 opened this issue on Jun 1, 2020 · 0 comments · Fixed by #3832

Assignees



Labels

bug parser

owl337 commented on Jun 1, 2020

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

```
var a = {
  "foo//b",
};
```

Output

```
ICE: Assertion 'context.status_flags & PARSER_SCANNING_SUCCESSFUL' failed at /home/JerryScript/jerryscript/jerry-core/parser/js/js-parser.c(parser_parse_source):2185.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted (core dumped)
```

Credits: This vulnerability is detected by chong from OWL337.

rerobika self-assigned this on Jun 2, 2020

rerobika added bug parser labels on Jun 2, 2020

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

Fix PropertyDefinition parsing in ObjectInitializer

da17c7d

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

Fix PropertyDefinition parsing in ObjectInitializer #3832

Merged

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

Fix PropertyDefinition parsing in ObjectInitializer

87197ce

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

Fix PropertyDefinition parsing in ObjectInitializer

659e923

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

Fix PropertyDefinition parsing in ObjectInitializer

3bf4b7c

dbatyai closed this as completed in #3832 on Jun 3, 2020

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

Fix PropertyDefinition parsing in ObjectInitializer (#3832)

4660bab

Assignees



Labels

bug parser

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix PropertyDefinition parsing in ObjectInitializer**
rerobika/jerryscript

2 participants

