

New issue

Jump to bottom

Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' in parser_parse_function_statement #3821

Closed owl337 opened this issue on May 31, 2020 · 0 comments · Fixed by #3838

Assignees



Labels

bug parser

owl337 commented on May 31, 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

```
function a") {
```

Output

```
ICE: Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at /home/JerryScript/jerryscript/jerry-core/parser/js/js-parser-
statm.c(parser_parse_function_statement):733.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted (core dumped)
```

Credits: This vulnerability is detected by chong from OWL337.

rerobika assigned dbatyai on Jun 2, 2020

rerobika added bug parser labels on Jun 2, 2020

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

Fix parsig function statements containing invalid tokens ...

f60bbb4

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

Fix parsig function statements containing invalid tokens ...

7579ae8

dbatyai mentioned this issue on Jun 3, 2020

Fix parsing function statements containing invalid tokens #3838

Merged

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

Fix parsig function statements containing invalid tokens ...

97b04cc

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

Fix parsig function statements containing invalid tokens ...

8c316c7

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

Fix parsing function statements containing invalid tokens ...


6effd1c


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

Fix parsing function statements containing invalid tokens ...

14dd68a

 rerobika closed this as completed in [#3838](#) on Jun 4, 2020

 rerobika pushed a commit that referenced this issue on Jun 4, 2020

 Fix parsing function statements containing invalid tokens ([#3838](#)) ...

✓ 1322e08

Assignees

 dbatyai

Labels

bug **parser**

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 Fix parsing function statements containing invalid tokens
dbatyai/jerascript

3 participants

