

New issue

Jump to bottom

# Assertion 'scope\_stack\_p > context\_p->scope\_stack\_p' in scanner\_literal\_is\_created #3823

Closed owl337 opened this issue on May 31, 2020 · 0 comments · Fixed by #3832

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 f ({"aba,a"})
{
}

Output

ICE: Assertion 'scope\_stack\_p > context\_p->scope\_stack\_p' failed at /home/JerryScript/jerryscript/jerry-core/parser/js/js-scanner-util.c(scanner\_literal\_is\_created):2510.
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 ... d1d83f9

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 ... da17c7d

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

 rerobika

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/jerrycript

2 participants

