Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' in parser_parse_function_arguments #3835

Closed owl337 opened this issue on Jun 3, 2020 · 0 comments · Fixed by #3832

Labels bug

owl337 commented on Jun 3, 2020

JerryScript revision

a56e31f

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 --stack-limit=50
```

Test case

```
fn_expr = {
"foo//b",
}

(function () {
 var a = [arguments];
})();
```

Output

```
ICE: Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at /home/JerryScript/jerry-core/parser/js/js-parser.c(parser_parse_function_arguments):1705.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted (core dumped)
```

Credits: This vulnerability is detected by chong from OWL337.

rerobika linked a pull request on Jun 3, 2020 that will close this issue

Fix PropertyDefinition parsing in ObjectInitializer #3832 Merged

rerobika added the bug label on Jun 3, 2020

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

Assignees

No one assigned

Labels

bug

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