

New issue

[Jump to bottom](#)

Assertion 'context_p->next_scanner_info_p->type ==
SCANNER_TYPE_FUNCTION' failed at
/home/ubuntu/fuzz/jerryscript/jerry-core/parser/js/js-
parser.c(parser_parse_function_arguments):1618 #4916

 Closed

cnitlrt opened this issue on Jan 2 · 0 comments · Fixed by [#4942](#)

Assignees



Labels

bug

cnitlrt commented on Jan 2

JerryScript commit hash

a6ab5e9

Build platform

Ubuntu 20.04 LTS

Build steps

```
./tools/build.py --clean --compile-flag=-fsanitize=address --lto=off --error-message=on --profile=es2015-  
subset --stack-limit=15 --debug --logging=on --line-info=on
```

poc

```
function test(proxyTarget) {  
    var {  
        proxy,  
        revoke  
    } = Proxy.revocable(proxyTarget, new Proxy({}, {  
        get: (target, propertyKey, receiver) {  
            revoke();  
        }  
    }));  
});
```

```
        return proxy;
    }

    Object.getPrototypeOf(test({}));
```





















assert log

```
ICE: Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at
/home/ubuntu/fuzz/jerryscript/jerry-core/parser/js/js-
parser.c(parser_parse_function_arguments):1618.
Error: ERR_FAILED_INTERNAL_ASSERTION
Aborted
```

asan log

```
AddressSanitizer:DEADLYSIGNAL
=====
==602568==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55cb2935a0c1 bp
0x7ffdb322746c sp 0x7ffdb32250a0 T0)
==602568==The signal is caused by a READ memory access.
==602568==Hint: address points to the zero page.
#0 0x55cb2935a0c0 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2d40c0)
#1 0x55cb2932cbce (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2a6bce)
#2 0x55cb2933ed63 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2b8d63)
#3 0x55cb2945e610 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3d8610)
#4 0x55cb294763dc (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f03dc)
#5 0x55cb2947ea5f (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f8a5f)
#6 0x55cb2947c741 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f6741)
#7 0x55cb2947ea8b (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f8a8b)
#8 0x55cb2947c741 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f6741)
#9 0x55cb2947ea8b (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3f8a8b)
#10 0x55cb2948623b (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x40023b)
#11 0x55cb29487623 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x401623)
#12 0x55cb294951f3 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x40f1f3)
#13 0x55cb2949a49b (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x41449b)
#14 0x55cb2933ef1a (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2b8f1a)
#15 0x55cb294925c5 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x40c5c5)
#16 0x55cb2949c035 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x416035)
#17 0x55cb2933b318 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2b5318)
#18 0x55cb29200f3d (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x17af3d)
#19 0x55cb290b7290 (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x31290)
#20 0x7f2801d550b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#21 0x55cb290c4c0d (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x3ec0d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/ubuntu/fuzz/jerryscript/build/bin/jerry+0x2d40c0)
==602568==ABORTING
```

-   **cniitlrl** changed the title ~~ICE: Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at /home/ubuntu/fuzz/jerryscript/jerry-core/parser/js/js-parser.c(parser_parse_function_arguments):1618~~ Assertion 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at /home/ubuntu/fuzz/jerryscript/jerry-core/parser/js/js-parser.c(parser_parse_function_arguments):1618 on Jan 2
-  **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 3
-  Fix lexer_expect_object_literal_id after [jerryscript-project#4841](#) ... ✓ ea284b8
-  **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 3
-  Fix lexer_expect_object_literal_id ... ✗ a7ab49d
-  **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 3
-  Fix lexer_expect_object_literal_id ... ✓ 4199f8e
-   **rerobika** assigned **mnegyokru** on Jan 4
-   **rerobika** added the **bug** label on Jan 4
-  **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 4
-  Fix lexer_expect_object_literal_id ... ✓ 8c64614
-   **mnegyokru** mentioned this issue on Jan 4
- Fix class static block opening brace parsing #4942**
-  Merged
-  **mnegyokru** added a commit to mnegyokru/jerryscript that referenced this issue on Jan 4
-  Fix class static block opening brace parsing ... ✓ aa8a364
-  This was referenced on Jan 4
- Use After Free at jerry-core/parser/js/js-lexer.c:3503 in lexer_compare_identifier_to_string #4917**

✓ Closed

Assertion 'scope_stack_p > context_p->scope_stack_p' failed at jerry-core/parser/js/js-scanner-util.c(scanner_literal_is_created):3112. #4918

✓ Closed

Assertion 'scope_stack_p >= context_p->scope_stack_p' failed at jerry-core/parser/js/js-parser-statm.c(parser_parse_function_statement):741. #4919

✓ Closed

Assertion 'context_p->token.type != LEXER_RIGHT_PAREN' failed at jerryscript/jerry-core/parser/js/js-parser-statm.c(parser_parse_for_statement_start):1605. #4922

✓ Closed

Assertion 'context_p->token.type == LEXER_LITERAL && (context_p->token.lit_location.type == LEXER_IDENT_LITERAL || context_p->token.lit_location.type == LEXER_STRING_LITERAL)' failed at jerryscript/jerry-core/parser/js/js-lexer.c(lexer_compare_literal_to_string):3696. #4923

✓ Closed

Assertion 'context_p->token.type == LEXER_RIGHT_BRACE || context_p->token.type == LEXER_ASSIGN || context_p->token.type == LEXER_COMMA' failed at jerryscript/jerry-core/parser/js/js-parser-expr.c(parser_parse_object_initializer):4178. #4926

✓ Closed

 mnegyokru added a commit to mnegyokru/jerryscript that referenced this issue on Jan 4



Fix class static block opening brace parsing ...

✓ 5e1fdd1

 rerobika mentioned this issue on Jan 4

Assertion 'context.status_flags & PARSE_SCANNING_SUCCESSFUL' failed at jerryscript/jerry-core/parser/js/js-parser.c(parser_parse_source):2348. #4929

✓ Closed

 dbatyai closed this as completed in [#4942](#) on Jan 10

 dbatyai pushed a commit that referenced this issue on Jan 10



Fix class static block opening brace parsing ([#4942](#)) ...

✓ f3a420b

Assignees

mnegyokru

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix class static block opening brace parsing**
mnegyokru/jerryscript

3 participants

