ASSERTION (pFuncBody->GetYieldRegister() == oldYieldRegister) failed in Js::DebugContext::RundownSourcesAndReparse #6453

Open owl337 opened this issue on Jun 1, 2020 · 0 comments

Labels Bug Debugger

owl337 commented on Jun 1, 2020 • edited

ChakraCore version:

version 1.12.0.0-beta

Build Commond

./build.sh --debug

OS

Ubuntu 16.04.6 LTS (Linux 4.4.0-142-generic x86_64)

Test case

```
function test0() {
  var func2 = (async (xsbazt = hkvvxr(x)) => [...[
        -2,
      ]]);
  var a = -191;
  func3(a);
}

function Run(){
    WScript.Echo('PASSED');
}


WScript.Attach(Run);
```

Output

```
ASSERTION 202914: (ChakraCore/lib/Runtime/Debug/DebugContext.cpp, line 359) pFuncBody->GetYieldRegister() == oldYieldRegister
 Failure: (pFuncBody->GetYieldRegister() == oldYieldRegister)
Illegal instruction
```

Credits: This vulnerability is detected by chong from OWL337.

👍 1

owl337 changed the title ~~DebugBreak in Js::DebugContext::RundownSourcesAndReparse~~ ASSERTION (pFuncBody->GetYieldRegister() == oldYieldRegister) failed in Js::DebugContext::RundownSourcesAndReparse on Jun 1, 2020

ppenzin added Bug Debugger labels on Jun 8, 2020

Assignees

No one assigned

Labels

Bug Debugger

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants