New issue

Jump to bottom

SEVG in ecma_deref_bigint #4402

Closed **owl337** opened this issue on Jan 2, 2021 · 0 comments · Fixed by #4421

Assignees

Labels **bug** **ecma builtins** **ES.next**

owl337 commented on Jan 2, 2021

JerryScript revision

`2faafa4`

Build platform

Ubuntu 18.04.5 LTS(Linux 4.15.0-119-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  --builddir=$PWD/build
```

Test case

```
var p = new Proxy(Function(), { get: function closure() { eval("o.p.y"); delete closure; return closure == arguments.callee && !(new String(undefined)); }});
Function.prototype.bind.call(p);
```

Output

```
ReferenceError: o is not defined
ASAN:DEADLYSIGNAL
=================================================================
==24756==ERROR: AddressSanitizer: SEGV on unknown address 0xbebebeb8 (pc 0x56782398 bp 0xff8c72d8 sp 0xff8c72b0 T0)
==24756==The signal is caused by a READ memory access.
    #0 0x56782397 in ecma_deref_bigint /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:1264
    #1 0x5677d2c5 in ecma_free_value /root/jerryscript/jerry-core/ecma/base/ecma-helpers-value.c:1147
    #2 0x567c10fc in ecma_gc_free_object /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:1742
    #3 0x567c1e68 in ecma_gc_run /root/jerryscript/jerry-core/ecma/base/ecma-gc.c:1898
    #4 0x5678385a in ecma_finalize /root/jerryscript/jerry-core/ecma/base/ecma-init-finalize.c:83
    #5 0x567acb1d in jerry_cleanup /root/jerryscript/jerry-core/api/jerry.c:256
    #6 0x567a7a9c in main /root/jerryscript/jerry-main/main-unix.c:324
    #7 0xf774af20 in __libc_start_main (/lib32/libc.so.6+0x18f20)
    #8 0x566473d0  (/root/jerryscript/build/bin/jerry+0x1d3d0)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/jerryscript/jerry-core/ecma/base/ecma-helpers.c:1264 in ecma_deref_bigint
==24756==ABORTING
```

Credits: Found by chong from OWL337.

rerobika self-assigned this on Jan 5, 2021

rerobika added the **bug** label on Jan 5, 2021

rerobika added a commit to rerobika/jerryscript that referenced this issue on Jan 5, 2021

`Bound function 'length' property should be early initialized` ··· `c8354e8`

rerobika mentioned this issue on Jan 5, 2021

Bound function 'length' property should be early initialized #4421

Merged

akosthekiss added **ecma builtins** **ES.next** labels on Jan 5, 2021

zherczeg closed this as completed in #4421 on Jan 7, 2021

zherczeg pushed a commit that referenced this issue on Jan 7, 2021

`Bound function 'length' property should be early initialized (#4421)` ··· ✓ `6dfd02a`

Assignees

rerobika

Labels

bug ecma builtins ES.next

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Bound function 'length' property should be early initialized
rerobika/jerryscript

3 participants