New issue

Jump to bottom

Stack Exhaustion (ecma_proxy_object_get, ecma_proxy_object_set) #3785

Closed nszetei opened this issue on May 23, 2020 · 3 comments · Fixed by #3796

Assignees

Labels bug

nszetei commented on May 23, 2020

JerryScript revision

6cd309b

Build platform

Ubuntu 20.04 LTS (Linux 5.4.0-31-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
```

Test cases

```
var v2 = {};
var v4 = new Proxy(Uint8Array,v2);
v4.__proto__ = v4;
v4[1] = 2;
```

```
var v1 = {};
var v3 = new Proxy(parseFloat,v1);
v3.__proto__ = v3;
var v6 = "aa".constructor;
var v7 = parseFloat & v6;
```

akosthekiss commented on May 23, 2020 Member

Could you please try whether you get SO even if you set a limit for the stack? (Note: You can use `--stack-limit` option when building the engine to limit the maximum amount of stack that the engine can use.)

nszetei commented on May 23, 2020 Author

> Could you please try whether you get SO even if you set a limit for the stack? (Note: You can use `--stack-limit` option when building the engine to limit the maximum amount of stack that the engine can use.)

Yes. Unlike #3783 here I got SO in both cases (e.g. with `--stack-limit=10`).

1

nszetei commented on May 23, 2020 Author

Just to have it grouped together, a PoC for `ecma_proxy_object_has` :

```
function main() {
var v1 = [13.37,13.37,13.37,13.37];
var v4 = {isExtensible:Infinity};
var v6 = new Proxy(WeakMap,v4);
v6.__proto__ = v1;
v1.__proto__ = v6;
with (v1) {
    valueOf = 0;
}
}
main();
```

dbatyai self-assigned this on May 25, 2020

dbatyai added the **bug** label on May 25, 2020

dbatyai added a commit to dbatyai/jerryscript that referenced this issue on May 25, 2020

`Add stack limit check to proxy operations` ··· ✕ `012b81c`

dbatyai mentioned this issue on May 25, 2020

Add stack limit check to proxy operations #3796

Merged

dbatyai added a commit to dbatyai/jerryscript that referenced this issue on May 25, 2020

`Add stack limit check to proxy operations` ··· ✕ `e2e4818`

dbatyai added a commit to dbatyai/jerryscript that referenced this issue on May 25, 2020

`Add stack limit check to proxy operations` ··· ✓ `a096da7`

zherczeg closed this as completed in #3796 on May 26, 2020

---

zherczeg pushed a commit that referenced this issue on May 26, 2020

`Add stack limit check to proxy operations (#3796)` ··· ✓ `15629e8`

ossy-szeged mentioned this issue on Jan 25, 2021

Fixes the Clang compiler caused deadloop issue #4530

Closed

Assignees

dbatyai

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Add stack limit check to proxy operations
dbatyai/jerryscript

3 participants