



[quickjs-devel] Re: Expected TypeError exception is not thrown

发件人: Fabrice Bellard <fabrice@bellard.org>

时 间: 2019年9月19日(星期四) 凌晨2:29

收件人: QuickJS <quickjs-devel@freelists.org>

Hi,

Although QuickJS behaves differently than the other engines you tested, it is not a bug. The specification says that `comparefn(a, a)` shall return 0 (reflexivity). Hence the engine is free to avoid calling `comparefn` in this case. In your test, `a = b = null`, hence `comparefn` is not called by QuickJS. You will check that QuickJS behaves correctly by using:

```
var NISLParameter1 = [null, 0];
```

Best regards,

Fabrice.

On 9/18/19 4:44 PM, Houyou Yao wrote:

```
> Hello,
> Expected TypeError exception is not thrown when running the statement
> "null.getValue()" in the compare function of
> Array.prototype.sort(comparefn).
> The detailed description is as follows:
>
> # version: quickjs-2019-09-01
>
> # Testcase:
> var NISLFuzzingFunc = function(loader) {
>   loader.sort(function(a, b) {
>     var value = a.getValue();
>   });
>   print(null.getValue());
> };
> var NISLParameter1 = [null, null];
> NISLFuzzingFunc(NISLParameter1);
>
> # Command:
> ./quickjs-2019-09-01/qjs testcase.js
>
```

> # Output:
> TypeError: value has no property
> at NISLFuzzingFunc (testcase.js:5)
> at <eval> (testcase.js:8)
>
> # Expected output:
> TypeError should be thrown on Line 3 instead of Line 5
>
> # Description:
> In the testcase above, QuickJS throws TypeError on Line 5 to indicate
> that accessing "null.getValue()" is illegal, but it does not throw
> exception on Line 3 as expected. When deleting the statement
> "print(null.getValue());" on Line 5, QuickJS throw no exception while
> other engines throw TypeError on Line 3, such as v8, spiderMonkey,
> javascriptCore, chakra.
>
> Is it a bug of QuickJS? Looking forward to your reply. Thank you
> very much!
>
> Best Regards,
> Houyou Yao
>
>