QQ邮箱 mail.qq.com

Re: [quickjs-devel] The delete operation does not meet the standard

发件人：Fabrice Bellard<fabrice@bellard.org>
时　间：2019年9月18日(星期三) 凌晨3:00
收件人：姚厚友<yaohouyou@qq.com>

Hi,

It will be fixed in the next release.

Best regards,

Fabrice.

On 9/16/19 3:33 AM, Houyou Yao wrote:
> Hello!
> I am very sorry to bother you, maybe you have already replied to
> this email, but I have not received it. I look forward to your reply
> again, and I hope that you can answer the following questions.
> Q1: Is it a bug of QuickJS?
> Q2: if Q1 is yes, will this bug be fixed in the future, or has it been
> fixed?
> Thank you very much!
>
>
>
> The following description is a possible issue for QuickJS:
>
> *version:* quickjs-2019-08-18
>
> *Testcase:*
> var NISLFuzzingFunc = function () {
> delete Array[0][1];
> };
> NISLFuzzingFunc();
>
> *Command:*
> ./ quickjs-2019-08-18/qjs testcase.js
>
> *Output:*
>
>
> *Expected output:*

> Throw TypeError on line 2
>
> *Description:*
> QuickJS will throw a TypeError when accessing the attribute of
> undefined, for example: "print(Array[0][1]);". In the testcase above,
> TypeError should be thrown on Line 2 according to ES standard, while
> QuickJS does not seem to do like this. Maybe, QuickJS ignored step 2 of
> the delete operation in the ES standard: "ReturnIfAbrupt(ref)".
> The reference of ECMAScript-262 standard is as follows:
> https://tc39.es/ecma262/#sec-delete-operator-runtime-semantics-evaluation
>
>
> Cheers,
> Houyou Yao
>
>
>