QQ邮箱 mail.qq.com

[quickjs-devel] Re: A bug about Number.prototype.toString

发件人：Fabrice Bellard<fabrice@bellard.org>
时　间：2019年12月14日(星期六) 晚上8:16
收件人：QuickJS<quickjs-devel@freelists.org>

Yes it is a known issue (the spec tells the result is implementation defined so QuickJS is still compliant !). It will be improved once the floating point to string conversion is reworked. 'qjsbn' does not have the problem because it uses libbf to do the conversion.

Best regards,

Fabrice.

On 12/11/19 2:13 AM, Houyou Yao wrote:
> # Version: quickjs-2019-10-27
>
> # Testcase:
> var NISLFuzzingFunc = function(a) {
>   var b = a.toString(16);
>   print(b);
> };
> var NISLParameter0 = 16.1;
> NISLFuzzingFunc(NISLParameter0);
>
> # Command:
> quickjs-2019-10-27/qjs testcase.js
>
> # Output:
> 16.1
>
> # Expected output:
> 10.19999999999a
>
> # Description:
> When calling Number.prototype.toString ([radix]), if the Number is
> not an integer, the output of QuickJS will be abnormal.