New issue

Jump to bottom

stack-overflow jsvar.c:74 in jsvGetNextSibling #2136

Closed Q1IQ opened this issue on Jan 29 · 1 comment

Q1IQ commented on Jan 29

Environment

```
MacOS Version : 11.5.2 (Intel)
Commit        : a8c74cbe557924dec90cc0da4f7a6a180a1a47d6
Version       : 2v11
```

Build

```
CFLAGS += -fsanitize=address -fno-omit-frame-pointer
```

Proof of concept

```
function main() {
    var foo = Int16Array(31860);
    var buf = foo.reduce(Array);
}
main();
```

Stack Dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==40754==ERROR: AddressSanitizer: stack-overflow on address 0x7ffee802dff0 (pc 0x0001073f2364 bp
0x7ffee802e010 sp 0x7ffee802dfe0 T0)
```

```
    #0 0x1073f2364 in jsvGetNextSibling jsvar.c:74
    #1 0x1073f7f47 in jsvFreePtr jsvar.c:553
    #2 0x1073f8ed4 in jsvUnLockFreeIfNeeded jsvar.c:723
    #3 0x1073f87d0 in jsvUnLock jsvar.c:735
    #4 0x1073f8047 in jsvFreePtr jsvar.c:569
    #5 0x1073f8ed4 in jsvUnLockFreeIfNeeded jsvar.c:723
    #6 0x1073f87d0 in jsvUnLock jsvar.c:735
    #7 0x1073f842a in jsvFreePtr jsvar.c:642
    #8 0x1073f8ed4 in jsvUnLockFreeIfNeeded jsvar.c:723
    #9 0x1073f87d0 in jsvUnLock jsvar.c:735
    #10 0x1073f8047 in jsvFreePtr jsvar.c:569
[···]
    #251 0x1073f8ed4 in jsvUnLockFreeIfNeeded jsvar.c:723
    #252 0x1073f87d0 in jsvUnLock jsvar.c:735
    #253 0x1073f842a in jsvFreePtr jsvar.c:642
    #254 0x1073f8ed4 in jsvUnLockFreeIfNeeded jsvar.c:723
    #255 0x1073f87d0 in jsvUnLock jsvar.c:735

SUMMARY: AddressSanitizer: stack-overflow jsvar.c:74 in jsvGetNextSibling
==40754==ABORTING
```

Credit

Q1IQ(**@Q1IQ**)

gfwilliams commented on Jan 31 — Member

Ok, thanks - so it's not an endless recursion problem, it's just that a datastructure that's linked very deep uses a lot of stack to free itself.

I'll add a stack overflow check is needed in the 'Free' code, which should at least stop this from failing - and then later a GC pass would clean up the remainder.

gfwilliams closed this as completed in 7744241 on Jun 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants