# Ruby - Bug #14894

## Segfault loading iseqs

07/03/2018 11:53 PM - sam.saffron (Sam Saffron)

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | | | |
| **Target version:** | | | |
| **ruby -v:** | | **Backport:** | 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN |

**Description**

Follow up on https://github.com/Shopify/bootsnap/issues/172

In particular:

https://gist.githubusercontent.com/SamSaffron/1fe47b86374823fb620a6a29c83538ec/raw/c7e7b8f9bd605ab066bd66258ec76eab6df7fdff/dump.txt

Seeing a segfault in Ruby trunk during ibf_load_iseq_each which is likely GC related.

To repro, check out Discourse and run bundle exec rails c happens one in N times.

This is looks GC related.

It may be triggered by bootsnap (and bootsnap's issue) here which appears to be handing around VALUE* so maybe one of these is not properly protected.

https://github.com/Shopify/bootsnap/blob/4d0b042b1f20e67ee7f05487cba0065fe4d80c91/ext/bootsnap/bootsnap.c#L723-L750

Issue does not appear to happen on 2.5.1 or lower

**Related issues:**

| | |
|---|---|
| Related to Ruby - Bug #14959: Writing a "link_to" method and a "url_helper" w... | **Closed** |

### History

**#1 - 06/19/2019 07:31 PM - jeremyevans0 (Jeremy Evans)**

*- Related to Bug #14959: Writing a "link_to" method and a "url_helper" with a request parameter under certain "if else" statement in Rails helper crashes with KERN_INVALID_ADDRESS at 0x0000000000000000 added*

**#2 - 06/19/2019 07:31 PM - jeremyevans0 (Jeremy Evans)**

*- Status changed from Open to Closed*