

Ruby - Bug #19339

Defining ivar on special constants with @ syntax causes segv

01/14/2023 09:02 PM - luke-gru (Luke Gruber)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
		Backport: 2.7: DONTNEED, 3.0: DONTNEED, 3.1: DONTNEED, 3.2: DONE
Description		
<pre>1.instance_eval do @a = 1 end</pre>		
There's a missing check at the top of vm_setivar_fastpath, should be:		
<pre>if (UNLIKELY(RB_SPECIAL_CONST_P(obj))) { // example code: 1.instance_eval { @a = 1 } rb_check_frozen(obj); // raise FrozenError, because it's always frozen return Qundef; }</pre>		

Associated revisions

Revision ed6fbb79e19bf401db0e85447fee955fd10a25c7 - 01/17/2023 09:51 AM - peterzhu2118 (Peter Zhu)

Fix crash when defining ivars on special constants

[Bug #19339]

Revision ed6fbb79e19bf401db0e85447fee955fd10a25c7 - 01/17/2023 09:51 AM - peterzhu2118 (Peter Zhu)

Fix crash when defining ivars on special constants

[Bug #19339]

Revision ed6fbb79 - 01/17/2023 09:51 AM - peterzhu2118 (Peter Zhu)

Fix crash when defining ivars on special constants

[Bug #19339]

Revision c0df0a85dec77a09308caddb1e1efd4d38fbf7b8 - 01/20/2023 08:01 AM - naruse (Yui NARUSE)

merge revision(s) ed6fbb79e19bf401db0e85447fee955fd10a25c7: [Backport #19339]

Fix crash when defining ivars on special constants

[Bug #19339]

```
test/ruby/test_variable.rb | 6 ++++++
vm_inshelper.c             | 5 +++++
2 files changed, 11 insertions(+)
```

Revision c0df0a85dec77a09308caddb1e1efd4d38fbf7b8 - 01/20/2023 08:01 AM - naruse (Yui NARUSE)

merge revision(s) ed6fbb79e19bf401db0e85447fee955fd10a25c7: [Backport #19339]

Fix crash when defining ivars on special constants

[Bug #19339]

```
test/ruby/test_variable.rb | 6 ++++++
vm_inshelper.c             | 5 +++++
2 files changed, 11 insertions(+)
```

Revision c0df0a85 - 01/20/2023 08:01 AM - naruse (Yui NARUSE)

merge revision(s) ed6fbb79e19bf401db0e85447fee955fd10a25c7: [Backport #19339]

Fix crash when defining ivars on special constants

[Bug #19339]

```
---
test/ruby/test_variable.rb | 6 ++++++
vm_insnhelper.c            | 5 +++++
2 files changed, 11 insertions(+)
```

History

#1 - 01/16/2023 02:34 PM - peterzhu2118 (Peter Zhu)

- Backport changed from 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN to 2.7: DONTNEED, 3.0: DONTNEED, 3.1: DONTNEED, 3.2: REQUIRED

Thank you for reporting this bug. I opened a PR with the fix here: <https://github.com/ruby/ruby/pull/7129>

#2 - 01/17/2023 09:57 AM - peterzhu2118 (Peter Zhu)

- Status changed from Open to Closed

Applied in changeset [git|ed6fbb79e19bf401db0e85447fee955fd10a25c7.](#)

Fix crash when defining ivars on special constants

[Bug [#19339](#)]

#3 - 01/24/2023 02:05 AM - naruse (Yui NARUSE)

- Backport changed from 2.7: DONTNEED, 3.0: DONTNEED, 3.1: DONTNEED, 3.2: REQUIRED to 2.7: DONTNEED, 3.0: DONTNEED, 3.1: DONTNEED, 3.2: DONE

ruby_3_2 c0df0a85dec77a09308caddb1e1efd4d38fbf7b8 merged revision(s) ed6fbb79e19bf401db0e85447fee955fd10a25c7.