

Ruby - Bug #20752

IO::Buffer#slice creates mutable IO::Buffer instance that points to readonly memory (e.g. frozen String)

09/18/2024 09:38 AM - hanazuki (Kasumi Hanazuki)

Status:Closed Priority:Normal Assignee:ioquatix (Samuel Williams) Target version: ruby -v:ruby 3.4.0dev (2024-09-18T02:16:22Z master 4797b0704a) +PRISM [x86_64-linux]	Backport:3.1: REQUIRED, 3.2: DONE, 3.3: DONE
Description <pre>irb(main):001> RUBY_DESCRIPTION.frozen? => true irb(main):002> IO::Buffer.for(RUBY_DESCRIPTION).set_string('perl', 0, 4) (irb):2:in 'IO::Buffer#set_string': Buffer is not writable! (IO::Buffer::AccessError) from (irb):2:in '<main>' from <internal:kernel>:191:in 'Kernel#loop' from -e:1:in '<main>' irb(main):003> IO::Buffer.for(RUBY_DESCRIPTION).slice.set_string('perl', 0, 4) => 4 irb(main):004> RUBY_DESCRIPTION => "perl 3.4.0dev (2024-09-18T02:16:22Z master 4797b0704a) +PRISM [x86_64-linux]" irb(main):001> IO::Buffer.for(NameError.name).slice.set_string('X', 0, 1) => 1 irb(main):002> NameError (irb):2:in '<main>': uninitialized constant NameError (XameError) from <internal:kernel>:191:in 'Kernel#loop' from -e:1:in '<main>'</pre>	

Associated revisions

Revision 637067440f74043c6d79fc649ab8acf1afea25a5 - 09/30/2024 11:39 AM - nobu (Nobuyoshi Nakada)

[Bug #20752] Slice of readonly IO::Buffer also should be readonly

Revision 637067440f74043c6d79fc649ab8acf1afea25a5 - 09/30/2024 11:39 AM - nobu (Nobuyoshi Nakada)

[Bug #20752] Slice of readonly IO::Buffer also should be readonly

Revision 63706744 - 09/30/2024 11:39 AM - nobu (Nobuyoshi Nakada)

[Bug #20752] Slice of readonly IO::Buffer also should be readonly

Revision 5777fe5ab57d6479326bdb21ef9a6b88ea1516dc - 10/18/2024 02:30 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

Revision 5777fe5ab57d6479326bdb21ef9a6b88ea1516dc - 10/18/2024 02:30 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

Revision 5777fe5a - 10/18/2024 02:30 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

Revision 12ea98e8c8af0ed6778aad26e7ec5f95e2c239e5 - 11/04/2024 10:38 PM - k0kubun (Takashi Kokubun)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

Revision 12ea98e8c8af0ed6778aad26e7ec5f95e2c239e5 - 11/04/2024 10:38 PM - k0kubun (Takashi Kokubun)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

Revision 12ea98e8 - 11/04/2024 10:38 PM - k0kubun (Takashi Kokubun)

merge revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5: [Backport #20752]

[Bug #20752] Slice of readonly `IO::Buffer` also should be readonly

History

#1 - 09/18/2024 10:00 AM - nobu (Nobuyoshi Nakada)

- Backport changed from 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN to 3.1: REQUIRED, 3.2: REQUIRED, 3.3: REQUIRED

It results in bus errors with 3.1 and 3.2.

```
$ ruby3.2 -e 'IO::Buffer.for(RUBY_DESCRIPTION).slice.set_string("perl", 0, 4)'  
-e:1: [BUG] Bus Error at 0x0000000100f08b18  
ruby 3.2.5 (2024-07-26 revision 31d0f1a2e7) [arm64-darwin23]
```

```
$ ruby3.1 -e 'IO::Buffer.for(RUBY_DESCRIPTION).slice(0, 8).set_string("perl", 0, 4)'  
-e:1: [BUG] Bus Error at 0x00000001039c7e38  
ruby 3.1.4p223 (2023-03-30 revision 957bb7cb81) [arm64-darwin23]
```

#2 - 09/18/2024 01:48 PM - hanazuki (Kasumi Hanazuki)

- Subject changed from *IO::Buffer#slice fails to copy readonly flag, allowing writes into frozen String* to *IO::Buffer#slice creates mutable IO::Buffer instance that points to readonly memory (e.g. frozen String)*

#3 - 09/30/2024 05:20 AM - mame (Yusuke Endoh)

- Assignee set to ioquatix (Samuel Williams)

#4 - 09/30/2024 12:00 PM - ioquatix (Samuel Williams)

The second example XameError is hilarious, what a great bug. Yes, this should be fixed.

#5 - 09/30/2024 12:07 PM - ioquatix (Samuel Williams)

Looks like @nobu (Nobuyoshi Nakada) already made a PR here: <https://github.com/ruby/ruby/pull/11735>

#6 - 10/01/2024 05:45 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

#7 - 10/18/2024 03:19 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 3.1: REQUIRED, 3.2: REQUIRED, 3.3: REQUIRED to 3.1: REQUIRED, 3.2: DONE, 3.3: REQUIRED

ruby_3_2 5777fe5ab57d6479326bdb21ef9a6b88ea1516dc merged revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5.

#8 - 11/04/2024 10:38 PM - k0kubun (Takashi Kokubun)

- Backport changed from 3.1: REQUIRED, 3.2: DONE, 3.3: REQUIRED to 3.1: REQUIRED, 3.2: DONE, 3.3: DONE

ruby_3_3 12ea98e8c8af0ed6778aad26e7ec5f95e2c239e5 merged revision(s) 637067440f74043c6d79fc649ab8acf1afea25a5.