Ruby - Bug #17661

IO#each will segfault when if file is closed inside an `each_byte` block

02/27/2021 12:45 AM - tenderlovemaking (Aaron Patterson)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.6: UNKNOWN, 2.7: REQUIRED, 3.0: DONE

Description

As reported here: https://twitter.com/asterite/status/1363487990203506689 when iterating through a file's contents with #each_byte, if the filehandle is closed inside of the block yielded to by #each byte, this condition is not detected, and a segmentation fault is thrown.

Repro:

```
file = http://File.open(__FILE__)
file.each_byte do |byte|
  p byte
  file.close
end
```

Proposed fix is here: https://github.com/ruby/ruby/pull/4217

Associated revisions

Revision 13939d61b4b69bd109c5f41303c79868d639fa44 - 06/27/2021 02:18 AM - nobu (Nobuyoshi Nakada)

Check if closed after each yield [Bug #17661]

Revision 13939d61b4b69bd109c5f41303c79868d639fa44 - 06/27/2021 02:18 AM - nobu (Nobuyoshi Nakada)

Check if closed after each yield [Bug #17661]

Revision 13939d61 - 06/27/2021 02:18 AM - nobu (Nobuyoshi Nakada)

Check if closed after each yield [Bug #17661]

Revision e6e25b794d8db52e1df85a02f28846ad7eb82d49 - 09/18/2021 07:07 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 13939d61b4b69bd109c5f41303c79868d639fa44: [Backport #17661]

```
    Check if closed after each yield [Bug #17661]

    ---
     io.c                 |  4 +++-
     test/ruby/test_io.rb | 36 ++++++++++++++++++++++++++++++++++++
     2 files changed, 39 insertions(+), 1 deletion(-)
```

Revision e6e25b794d8db52e1df85a02f28846ad7eb82d49 - 09/18/2021 07:07 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 13939d61b4b69bd109c5f41303c79868d639fa44: [Backport #17661]

```
    Check if closed after each yield [Bug #17661]

    ---
     io.c                 |  4 +++-
     test/ruby/test_io.rb | 36 ++++++++++++++++++++++++++++++++++++
     2 files changed, 39 insertions(+), 1 deletion(-)
```

Revision e6e25b79 - 09/18/2021 07:07 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 13939d61b4b69bd109c5f41303c79868d639fa44: [Backport #17661]

```
    Check if closed after each yield [Bug #17661]
```

```
 ---
  io.c                 |  4 +++-
  test/ruby/test_io.rb | 36 ++++++++++++++++++++++++++++++++++++
  2 files changed, 39 insertions(+), 1 deletion(-)
```

History

#1 - 02/27/2021 02:46 AM - xtkoba (Tee KOBAYASHI)

Probably 's|http://||' to the reproducer?

#2 - 03/07/2021 12:55 AM - wyhaines (Kirk Haines)

Aaron filed this bug on my behalf, as I was having issues with my account. Those issues appear to be issues no more, however.

In the interest of having details appear in the issue tracker and not just on GitHub, I'll reiterate the description of the fix:

I have fixed the problem by adding a check inside the inner loop that iterates over the filehandle read buffer, and I have added a spec that will both expose the bug in an unfixed ruby, and pass in a fixed ruby.

The bug exists on every build of Ruby that I have available on my systems, and in looking at the history of io.c, it likely exists all the way back to 1.9.1.

#3 - 06/27/2021 02:38 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset git|13939d61b4b69bd109c5f41303c79868d639fa44.

Check if closed after each yield [Bug #17661]

#4 - 06/27/2021 02:45 AM - nobu (Nobuyoshi Nakada)

Moved the check just after rb_yield.
And I found that each_codepoint also had a similar bug.
@wyhaines (Kirk Haines) Could you add a spec for the method?

#5 - 09/12/2021 06:53 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN to 2.6: UNKNOWN, 2.7: REQUIRED, 3.0: REQUIRED

#6 - 09/18/2021 07:51 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.6: UNKNOWN, 2.7: REQUIRED, 3.0: REQUIRED to 2.6: UNKNOWN, 2.7: REQUIRED, 3.0: DONE

ruby_3_0 e6e25b794d8db52e1df85a02f28846ad7eb82d49 merged revision(s) 13939d61b4b69bd109c5f41303c79868d639fa44.