Ruby - Bug #17117

Corruption in ARGF.inplace

08/11/2020 08:02 PM - peterzhu2118 (Peter Zhu)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.8.0dev (2020-08-11T19:09:12Z inplace-str-corrup.. 16d72713d2) [x86_64-darwin19]	**Backport:**	2.5: REQUIRED, 2.6: REQUIRED, 2.7: REQUIRED

Description

Extension string stored in ARGF.inplace is created using an api designed for C string constants to create a Ruby string that points at another Ruby string. When the original string is swept, the extension string gets corrupted.

Reproduction script (on MacOS):

```
#!/usr/bin/ruby -pi.bak

BEGIN {
  GC.start(full_mark: true)
  arr = []
  1000000.times do |x|
    arr << "fooo#{x}"
  end
}

puts "hello"
```

Fix PR on GitHub

Reproduction

1. Assuming you have the above script in a file called test.rb.
2. Create a file called foo.txt with contents foo.
3. Run ruby test.rb foo.txt.

Expected behaviour

foo.txt with contents hello\nfoo and foo.txt.bak with contents foo.

Actual behavior

foo.txt with contents hello\nfoo and foo.txto121 with contents foo.

History

#1 - 08/11/2020 08:14 PM - peterzhu2118 (Peter Zhu)

- Description updated

#2 - 08/12/2020 09:47 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

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