

Ruby - Bug #20239

Segmentation fault when using Regex on a large String

02/06/2024 10:23 AM - martinsp (Martins Polakovs)

Status:	Closed	Backport: 3.2: DONE, 3.3: DONE
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.3.0 (2023-12-25 revision 5124f9ac75) [aarch64-linux]	
Description		
Since v3.2.0 ruby crashes with segmentation fault on the following script with a [BUG] Segmentation fault at ...		
<pre>require "rbconfig/sizeof" ("\u{0101}" + "a" * RbConfig::LIMITS["INT_MAX"] + "b").match(/b/)</pre>		
Crash can be reproduced on the following ruby versions:		
• ruby 3.2.0 (2022-12-25 revision a528908271) [aarch64-linux] • ruby 3.2.3 (2024-01-18 revision 52bb2ac0a6) [aarch64-linux] • ruby 3.3.0 (2023-12-25 revision 5124f9ac75) [aarch64-linux]		
ruby 3.1.4p223 (2023-03-30 revision 957bb7cb81) [aarch64-linux] works as expected		
It seems that call to enclen inside str_lower_case_match returns negative offset in this case		
https://bugs.ruby-lang.org/projects/ruby-master/repository/git/revisions/v3_3_0/entry/regexec.c#L4180		

Associated revisions

Revision 75aaeb35b82da26359b9418d2963384d0c55839c - 02/07/2024 06:14 AM - nobu (Nobuyoshi Nakada)

[Bug #20239] Fix overflow at down-casting

Revision 75aaeb35b82da26359b9418d2963384d0c55839c - 02/07/2024 06:14 AM - nobu (Nobuyoshi Nakada)

[Bug #20239] Fix overflow at down-casting

Revision 75aaeb35 - 02/07/2024 06:14 AM - nobu (Nobuyoshi Nakada)

[Bug #20239] Fix overflow at down-casting

Revision 2b35d80834f14011f7d313f8fac7855dc9949f70 - 07/06/2024 06:55 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

Revision 2b35d80834f14011f7d313f8fac7855dc9949f70 - 07/06/2024 06:55 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

Revision 2b35d808 - 07/06/2024 06:55 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

Revision df8a08fb6a1f173a9c25db15fbe390096f39c2ff - 07/08/2024 11:04 PM - k0kubun (Takashi Kokubun)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

Revision df8a08fb6a1f173a9c25db15fbe390096f39c2ff - 07/08/2024 11:04 PM - k0kubun (Takashi Kokubun)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

Revision df8a08fb - 07/08/2024 11:04 PM - k0kubun (Takashi Kokubun)

merge revision(s) 75aaeb35b82da26359b9418d2963384d0c55839c: [Backport #20239]

[Bug #20239] Fix overflow at down-casting

History

#1 - 02/07/2024 06:44 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset [git|75aaeb35b82da26359b9418d2963384d0c55839c](#).

[Bug [#20239](#)] Fix overflow at down-casting

#2 - 07/06/2024 06:50 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 3.0: UNKNOWN, 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN to 3.2: REQUIRED, 3.3: REQUIRED

#3 - 07/06/2024 07:19 AM - nagachika (Tomoyuki Chikanaga)

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

ruby_3_2 [2b35d80834f14011f7d313f8fac7855dc9949f70](#) merged revision(s) [75aaeb35b82da26359b9418d2963384d0c55839c](#).

#4 - 07/08/2024 11:04 PM - k0kubun (Takashi Kokubun)

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

ruby_3_3 [df8a08fb6a1f173a9c25db15fbe390096f39c2ff](#) merged revision(s) [75aaeb35b82da26359b9418d2963384d0c55839c](#).