Ruby master - Bug #11001

2.2.1 Segmentation fault in reserve_stack() function.

03/25/2015 02:04 PM - kiyoka (Kiyoka Nishiyama)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]	**Backport:**	2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: UNKNOWN

Description

SEGV depends on stack limit size with 'ulimit -s ' .

This shell script [ulimit_change_test.sh] can reproduce SEGV on my Debian environment.
my Linux environment is Debian/GNU Linux 7.8.
But, I cannot reproduce this SEGV on Amazon Linux environment.

result on Debian 7.8

```
 $ /tmp/ulimit_change_test.sh
8515
/tmp/ulimit_change_test.sh: 3 : 20470 Segmentation fault      ./ruby --version
8514
/tmp/ulimit_change_test.sh: 3 : 20471 Segmentation fault      ./ruby --version
8513
/tmp/ulimit_change_test.sh: 3 : 20472 Segmentation fault      ./ruby --version
8512
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8511
/tmp/ulimit_change_test.sh: 3 : 20475 Segmentation fault      ./ruby --version
8510
/tmp/ulimit_change_test.sh: 3 : 20476 Segmentation fault      ./ruby --version
8509
/tmp/ulimit_change_test.sh: 3 : 20477 Segmentation fault      ./ruby --version
8508
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8507
/tmp/ulimit_change_test.sh: 3 : 20480 Segmentation fault      ./ruby --version
8506
/tmp/ulimit_change_test.sh: 3 : 20481 Segmentation fault      ./ruby --version
8505
/tmp/ulimit_change_test.sh: 3 : 20482 Segmentation fault      ./ruby --version
8504
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8503
/tmp/ulimit_change_test.sh: 3 : 20485 Segmentation fault      ./ruby --version
8502
/tmp/ulimit_change_test.sh: 3 : 20486 Segmentation fault      ./ruby --version
8501
/tmp/ulimit_change_test.sh: 3 : 20487 Segmentation fault      ./ruby --version
8500
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8499
/tmp/ulimit_change_test.sh: 3 : 20490 Segmentation fault      ./ruby --version
8498
/tmp/ulimit_change_test.sh: 3 : 20491 Segmentation fault      ./ruby --version
8497
/tmp/ulimit_change_test.sh: 3 : 20492 Segmentation fault      ./ruby --version
8496
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8495
/tmp/ulimit_change_test.sh: 3 : 20495 Segmentation fault      ./ruby --version
```

```
8494
/tmp/ulimit_change_test.sh: 3 □: 20496 Segmentation fault      ./ruby --version
8493
/tmp/ulimit_change_test.sh: 3 □: 20497 Segmentation fault      ./ruby --version
8492
ruby 2.2.1p85 (2015-02-26 revision 49769) [x86_64-linux]
8491
/tmp/ulimit_change_test.sh: 3 □: 20500 Segmentation fault      ./ruby --version
8490
/tmp/ulimit_change_test.sh: 3 □: 20501 Segmentation fault      ./ruby --version
8489
/tmp/ulimit_change_test.sh: 3 □: 20502 Segmentation fault      ./ruby --version
 $
```

This SEGV occurs in reserve_stack() function.
I suspect that the buf[0x100] size is too small for margin.
I attached patch to fix it.

Related issues:

Related to Ruby master - Bug #11030: Ruby 2.2.1 fails to compile with harden...	**Closed**

History

#1 - 06/04/2015 01:52 AM - william.l. (William L. L.)

I also run into the bug too.

```
william@debianbox:~/talentlines/webui$ lsb_release -da
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 7.7 (wheezy)
Release:    7.7
Codename:   wheezy
william@debianbox:~/talentlines/webui$ uname -a
Linux debianbox 3.2.0-4-amd64 #1 SMP Debian 3.2.63-2+deb7u1 x86_64 GNU/Linux

william@debianbox:~/talentlines/webui$ ulimit -s 8191
william@debianbox:~/talentlines/webui$ ruby -v
Segmentation fault

william@debianbox:~/talentlines/webui$ ulimit -s 8000
william@debianbox:~/talentlines/webui$ ruby -v
ruby 2.2.2p95 (2015-04-13 revision 50295) [x86_64-linux]
```

#2 - 06/04/2015 09:45 AM - nobu (Nobuyoshi Nakada)

- Related to Bug #11030: Ruby 2.2.1 fails to compile with hardened GCC added

#3 - 06/04/2015 09:49 AM - nobu (Nobuyoshi Nakada)

- Description updated

- Status changed from Open to Feedback

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: UNKNOWN

Does it happen with recent versions?

#4 - 06/27/2015 04:49 AM - kubo (Takehiro Kubo)

Same issue with recent ruby versions on Ubuntu 12.04.

I tried it with recent OS versions and found that

- Ubuntu 12.04 - Segmentation fault
- Ubuntu 12.10 - Segmentation fault
- Ubuntu 13.04 - No problem
- Ubuntu 14.04 - No problem
- Ubuntu 15.04 - No problem
- Debian 8.1 - No problem

IMO, this may be an issue of OS, not of ruby.

#5 - 06/27/2015 06:08 AM - normalperson (Eric Wong)

kubo@jiubao.org wrote:

> IMO, this may be an issue of OS, not of ruby.

Fwiw, valgrind chokes here, too.

I tested valgrind 3.9.0 on CentOS 7.0 and also backported to
Debian 7.0 (wheezy).

I comment reserve_stack out when I'm debugging other problems
with valgrind.

#6 - 06/27/2015 11:38 PM - ko1 (Koichi Sasada)

On 2015/06/27 15:08, Eric Wong wrote:

> Fwiw, valgrind chokes here, too.

Try it before valgrind.

$ ulimit -s unlimited

--
// SASADA Koichi at atdot dot net

#7 - 06/28/2015 01:33 AM - nobu (Nobuyoshi Nakada)

Takehiro Kubo wrote:

> IMO, this may be an issue of OS, not of ruby.

Any criteria where works on or not?
Runtime kernel versions?

#8 - 06/28/2015 05:26 AM - kubo (Takehiro Kubo)

> Any criteria where works on or not?
> Runtime kernel versions?

Segmentaion fault

- Ubuntu 12.04 - kernel 3.2+
- Ubuntu 12.10 - kernel 3.5
- Debian 7.7 - kernel 3.2.63
- Debian 7.8 - kernel 3.4.105

No problem

- Ubuntu 13.04 - kernel 3.8
- Ubuntu 14.04 - kernel 3.13 or 3.16 (I deleted the VM. I don't know which is used.)
- Ubuntu 15.04 - kernel 3.19.3
- Debian 8.1 - kernel 3.16.7

Ubuntu
https://en.wikipedia.org/wiki/List_of_Ubuntu_releases#Table_of_versions
Debian 7.7
https://www.phoronix.com/scan.php?page=news_item&px=MTgxODY
Debian 7.8
http://news.softpedia.com/news/Debian-7-8-Arrives-with-Security-Fixes-and-Updated-Linux-Kernel-469629.shtml
Debian 8.1
http://news.softpedia.com/news/Debian-GNU-Linux-8-1-Jessie-Officially-Released-483592.shtml

On Ubuntu 12.04, stack size in emacs shell buffer is 8515 and
ruby gets segmentation fault. So I put 'ulimit -Ss 8192' in .bashrc
for workaround. (stack size in gnome-terminal is 8192.)

#9 - 07/23/2019 04:59 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Feedback to Closed

Files

0001-Bugfix-patch-of-reserve_stack-function.patch	720 Bytes	03/25/2015	kiyoka (Kiyoka Nishiyama)
ulimit_change_test.sh	211 Bytes	03/25/2015	kiyoka (Kiyoka Nishiyama)