Ruby trunk - Bug #5508

Is BigDecimal really not $SAFE?

10/30/2011 12:26 AM - angdraug (Dmitry Borodaenko)

Status:	Closed		
Priority:	Normal		
Assignee:	mrkn (Kenta Murata)		
Target version:	2.0.0		
ruby -v:	ruby 1.9.3dev (2011-09-23 revision 33323) [x86_64-linux]	**Backport:**	

Description

Why does BigDecimal call SafeStringValue?

irb(main):001:0> $SAFE = 1; BigDecimal.new('1'.taint)
SecurityError: Insecure operation - new
from (irb):1:in new'
from (irb):1
from /usr/bin/irb:12:in'

Compare with:

irb(main):001:0> $SAFE = 1; i = '1'.taint.to_i
=> 1
irb(main):002:0> i.tainted?
=> false

I think it makes a lot more sense to validate the input within BigDecimal, rather than validate and untaint the string before passing it to BigDecimal.new().

Associated revisions

Revision 1fec21fe - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@38147 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

Revision 38147 - 12/02/2012 03:09 PM - mrkn (Kenta Murata)

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]

History

#1 - 11/01/2011 12:56 PM - mrkn (Kenta Murata)

- Assignee set to mrkn (Kenta Murata)

- Target version set to 2.0.0

#2 - 03/18/2012 06:46 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

#3 - 12/03/2012 12:09 AM - mrkn (Kenta Murata)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r38147.
Dmitry, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/bigdecimal/bigdecimal.c (BigDecimal_new): stop checking string taintness. [Bug #5508] [ruby-core:40510]