Ruby trunk - Bug #5173

[PATCH] json/generator: prevent GC of temporary strings

08/09/2011 10:45 AM - normalperson (Eric Wong)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	2.0.0		
ruby -v:	ruby 1.9.4dev (2011-08-07 trunk 32885) [x86_64-linux]	**Backport:**	

Description

ext/json/generator/generator.c: prevent GC of temporary strings

We need to guard temporary strings from being collected while we append to the JSON buffer (which may allocate memory). The RSTRING_PAIR macro is dangerous since it preserves no pointer to the original string VALUE, allowing GC to reap the object while we're still using the (C) string pointer.

The included test case shows data corruption with large Bignums without this fix.

If you prefer git pull: git pull git://bogomips.org/ruby json-gc-guard

Associated revisions

Revision b14c060d - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@33122 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 33122 - 08/30/2011 02:23 AM - naruse (Yui NARUSE)

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Revision 510f6dc7 - 08/30/2011 02:25 AM - naruse (Yui NARUSE)

merge revision(s) 33122:

```
* ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1).
  [Bug #5173] [ruby-core:38866]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@33123 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 08/09/2011 11:23 AM - nobu (Nobuyoshi Nakada)

=begin
The implementation of json/generator seems quite naive.
I found a couple of severe bugs in several minutes.

$ ./ruby -rjson -e 'class Bignum;def to_s;end;end; p JSON::Ext::Generator::State.new.generate(1<<64)'
-e:1: [BUG] Bus Error

$ ./ruby -rjson -e 'class << (a = ""); def to_s;self;end; undef to_json; end; p JSON::Ext::Generator::State.new.generate(a)'
-e:0: stack level too deep (SystemStackError)

Anyway, JSON issues need to be reported to the upstream.
=end

#2 - 08/09/2011 12:11 PM - naruse (Yui NARUSE)

Nobuyoshi Nakada wrote:

> Anyway, JSON issues need to be reported to the upstream.

The upstream is https://github.com/flori/json

#3 - 08/09/2011 01:23 PM - normalperson (Eric Wong)

Nobuyoshi Nakada nobu@ruby-lang.org wrote:

> =begin
> The implementation of json/generator seems quite naive.

Yeah :< I don't know why any of the fbuffer code exists since rb_str_*
provides that functionality already...

> $ ./ruby -rjson -e 'class Bignum;def to_s;end;end; p JSON::Ext::Generator::State.new.generate(1<<64)'
> -e:1: [BUG] Bus Error

I made it raise TypeError in
http://bogomips.org/ruby-json.git/commit/?id=40869aa9fc8ab194813b8

> $ ./ruby -rjson -e 'class << (a = ""); def to_s;self;end; undef to_json; end; p JSON::Ext::Generator::State.new.generate(a)'
> -e:0: stack level too deep (SystemStackError)

Haven't gotten to this one, yet. Can you fix or report? Maybe I'll
have time tomorrow...

> Anyway, JSON issues need to be reported to the upstream.

I've ported the changes to the standalone json gem and
updated https://github.com/flori/json/issues/46 with links
to my repos.

--
Eric Wong

#4 - 08/30/2011 11:23 AM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r33122.
Eric, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/json: Merge json gem 1.5.4+ (2149f4185c598fb97db1). [Bug #5173] [ruby-core:38866]

Files

0001-ext-json-generator-generator.c-prevent-GC-for-tempor.patch	3.64 KB	08/09/2011	normalperson (Eric Wong)