<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>2.0.0</td>
</tr>
<tr>
<td>Backport:</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-ext-json-generator-generator.c-prevent-GC-for-tempor.patch</td>
<td>3.64KB</td>
<td>08/09/2011</td>
<td>normalperson (Eric Wong)</td>
</tr>
</tbody>
</table>