Ruby master - Bug #16698
Backport security fix for CVE-2020-10663

03/19/2020 05:40 PM - jeremyevans0 (Jeremy Evans)

| Status: | Closed |
| Priority: | Normal |
| Assignee: | |
| Target version: | |
| ruby -v: | Backport: 2.4: DONE, 2.5: DONE, 2.6: DONE, 2.7: DONTNEED |

Description
As announced at [https://www.ruby-lang.org/en/news/2020/03/19/json-dos-cve-2020-10663/](https://www.ruby-lang.org/en/news/2020/03/19/json-dos-cve-2020-10663/), you can upgrade the JSON gem to 2.3.0 to work around the security issue. However, that brings in new features and not just the security fix. The security issue itself is easy to fix in older ruby versions, and I think the next releases of Ruby 2.4, 2.5, and 2.6 should contain just this security fix without a JSON version upgrade. I'm not sure if we plan a security release of Ruby 2.4 before it goes fully out of support, but I think we should have one.

Attached is a patch for ruby 2.6. It applies cleanly to ruby 2.4 and 2.5 (with some offsets).

Associated revisions
Revision b379ec8d8 - 03/30/2020 10:22 PM - usa (Usaku NAKAMURA)
merge revision(s) 36e9ed7fe6eb2d14becf6c52452e4ab16e4bf01: [Backport #16698]

  backport 80b5a0ff2a7709367178f29d4eb1c54122b1c27 partially as a security fix for CVE-2020-10663. The patch was provided by Jeremy Evans.

  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67869 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 67869 - 03/30/2020 10:22 PM - usa (Usaku NAKAMURA)
merge revision(s) 36e9ed7fe6eb2d14becf6c52452e4ab16e4bf01: [Backport #16698]

  backport 80b5a0ff2a7709367178f29d4eb1c54122b1c27 partially as a security fix for CVE-2020-10663. The patch was provided by Jeremy Evans.

  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67869 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 68180523 - 03/31/2020 10:51 AM - usa (Usaku NAKAMURA)
merge revision(s) 36e9ed7fe6eb2d14becf6c52452e4ab16e4bf01: [Backport #16698]

  backport 80b5a0ff2a7709367178f29d4eb1c54122b1c27 partially as a security fix for CVE-2020-10663. The patch was provided by Jeremy Evans.

  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@67873 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 67873 - 03/31/2020 10:51 AM - usa (Usaku NAKAMURA)
merge revision(s) 36e9ed7fe6eb2d14becf6c52452e4ab16e4bf01: [Backport #16698]

  backport 80b5a0ff2a7709367178f29d4eb1c54122b1c27 partially as a security fix for CVE-2020-10663. The patch was provided by Jeremy Evans.

  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67869 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History
#1 - 03/20/2020 08:13 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: REQUIRED, 2.7: DONTNEED to 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE, 2.7: DONTNEED
Backported into ruby_2_6 at r67856.
Thank you for providing a clean patch.

#2 - 03/30/2020 10:22 PM - usa (Usaku NAKAMURA)
- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE, 2.7: DONTNEED to 2.4: REQUIRED, 2.5: DONE, 2.6: DONE, 2.7: DONTNEED

ruby_2_5 r67869 merged revision(s) 36e9ed71ef6eb2d14becf8c52452e4ab16e4bf01.

#3 - 03/31/2020 10:51 AM - usa (Usaku NAKAMURA)
- Backport changed from 2.4: REQUIRED, 2.5: DONE, 2.6: DONE, 2.7: DONTNEED to 2.4: DONE, 2.5: DONE, 2.6: DONE, 2.7: DONTNEED

ruby_2_4 r67873 merged revision(s) 36e9ed71ef6eb2d14becf8c52452e4ab16e4bf01.

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruby-2-6-json-cve-2020-10663.patch</td>
<td>1.05 KB</td>
<td>03/19/2020</td>
<td>jeremyevans0 (Jeremy Evans)</td>
</tr>
</tbody>
</table>