Backport21 - Backport #9482
backport r44809 and r44811
02/05/2014 12:05 AM - hsbt (Hiroshi SHIBATA)

| Status:     | Closed          |
| Priority:   | Normal          |
| Assignee:   | naruse (Yui NARUSE) |

Description
ref. CVE-2013-6393

Associated revisions
Revision 2d9d5c67 - 02/24/2014 04:24 AM - naruse (Yui NARUSE)
merge revision(s) 44809,44811,44813,44815,44816,44817,44818,44918,45003: [Backport #9482]

* ext/psych/yaml/emitter.c: merge libyaml 0.1.5
* ext/psych/yaml/loader.c: ditto
* ext/psych/yaml/parser.c: ditto
* ext/psych/yaml/reader.c: ditto
* ext/psych/yaml/scanner.c: ditto
* ext/psych/yaml/writer.c: ditto
* ext/psych/yaml/yaml_private.h: ditto
* ext/psych/lib/psych.rb: New release of psych.
* ext/psych/psych.gemspec: ditto

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@45160 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 45160 - 02/24/2014 04:24 AM - naruse (Yui NARUSE)
merge revision(s) 44809,44811,44813,44815,44816,44817,44818,44918,45003: [Backport #9482]

* ext/psych/yaml/emitter.c: merge libyaml 0.1.5
* ext/psych/yaml/loader.c: ditto
* ext/psych/yaml/parser.c: ditto
* ext/psych/yaml/reader.c: ditto
* ext/psych/yaml/scanner.c: ditto
* ext/psych/yaml/writer.c: ditto
* ext/psych/yaml/yaml_private.h: ditto
* ext/psych/lib/psych.rb: New release of psych.
* ext/psych/psych.gemspec: ditto

History
#1 - 02/05/2014 01:57 AM - naruse (Yui NARUSE)
- Status changed from Open to Rejected

The fix seems half-baked

#2 - 02/06/2014 11:08 PM - postmodern (Hal Brodigan)
The short-term solution would be to backport the updates to psych's vendored libyaml 0.1.4. The long-term solution is to cease vendoring libyaml and compile against the system's libyaml. Eitherway, I prefer that Ruby does not ship with vulnerable code. ;)

04/05/2020
#3 - 02/09/2014 04:06 PM - nagachika (Tomoyuki Chikanaga)
Just for reference, There are following changesets, r44813, r44815, r44816, r44817 and r44818.

#4 - 02/14/2014 07:44 AM - naruse (Yui NARUSE)
- Status changed from Rejected to Assigned

#5 - 02/19/2014 06:39 AM - naruse (Yui NARUSE)
44918,45003

#6 - 02/24/2014 04:24 AM - naruse (Yui NARUSE)
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

Applied in changeset r45160.

merge revision(s) 44809,44811,44813,44815,44816,44817,44818,44918,45003: [Backport #9482]

* ext/psych/yaml/emitter.c: merge libyaml 0.1.5
* ext/psych/yaml/loader.c: ditto
* ext/psych/yaml/parser.c: ditto
* ext/psych/yaml/reader.c: ditto
* ext/psych/yaml/scanner.c: ditto
* ext/psych/yaml/writer.c: ditto
* ext/psych/yaml/yaml_private.h: ditto
* ext/psych/lib/psych.rb: New release of psych.
* ext/psych/psych.gemspec: ditto