

Ruby - Bug #11760

Encoding is tainted unexpectedly by Marshal.load

12/02/2015 06:26 AM - nobu (Nobuyoshi Nakada)

Status:	Closed	Backport: 2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	r52850	
Description By Marshal.loading tainted source, Encoding object will be tainted.		
code to reproduce <pre>e = Encoding::UTF_8 p e.tainted? p e == Marshal.load(Marshal.dump(e).taint) p e.tainted?</pre>		
expected results false, true, and false		
actual results false, true, and true		

Associated revisions

Revision 2a66cc554db6263bc04c804ad62750497c26a772 - 12/02/2015 07:27 AM - nobu (Nobuyoshi Nakada)

encoding.c: defer finding encoding

- encoding.c (enc_m_loader): defer finding encoding object not to be infected by marshal source. [ruby-core:71793] [Bug #11760]
- marshal.c (r_object0): enable compatible loader on USERDEF class. the loader function is called with the class itself, instead of an allocated object, and the loaded data.
- marshal.c (compat_allocator_table): initialize compat_allocator_tbl on demand.
- object.c (rb_undefined_alloc): extract from rb_obj_alloc.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 2a66cc55 - 12/02/2015 07:27 AM - nobu (Nobuyoshi Nakada)

encoding.c: defer finding encoding

- encoding.c (enc_m_loader): defer finding encoding object not to be infected by marshal source. [ruby-core:71793] [Bug #11760]
- marshal.c (r_object0): enable compatible loader on USERDEF class. the loader function is called with the class itself, instead of an allocated object, and the loaded data.
- marshal.c (compat_allocator_table): initialize compat_allocator_tbl on demand.
- object.c (rb_undefined_alloc): extract from rb_obj_alloc.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52856 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f0680bdee869d37c0b654d0226ae665e6adc934e - 12/08/2015 02:51 AM - U.Nakamura

merge revision(s) 52856,52906: [Backport #11760]

```
* encoding.c (enc_m_loader): defer finding encoding object not to
```

be infected by marshal source. [ruby-core:71793] [Bug #11760]

* marshal.c (r_object0): enable compatible loader on USERDEF
class. the loader function is called with the class itself,
instead of an allocated object, and the loaded data.

* marshal.c (compat_allocator_table): initialize
compat_allocator_tbl on demand.

* object.c (rb_undefined_alloc): extract from rb_obj_alloc.

* marshal.c (compat_allocator_table): initialize

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@52933 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f0680bde - 12/08/2015 02:51 AM - U.Nakamura

merge revision(s) 52856,52906: [Backport #11760]

* encoding.c (enc_m_loader): defer finding encoding object not to
be infected by marshal source. [ruby-core:71793] [Bug #11760]

* marshal.c (r_object0): enable compatible loader on USERDEF
class. the loader function is called with the class itself,
instead of an allocated object, and the loaded data.

* marshal.c (compat_allocator_table): initialize
compat_allocator_tbl on demand.

* object.c (rb_undefined_alloc): extract from rb_obj_alloc.

* marshal.c (compat_allocator_table): initialize

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@52933 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision bd4364acb13fbf03e80dcf83a5e3b5d29410b0cc - 12/08/2015 04:44 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52856,52906: [Backport #11760]

* encoding.c (enc_m_loader): defer finding encoding object not to
be infected by marshal source. [ruby-core:71793] [Bug #11760]

* marshal.c (r_object0): enable compatible loader on USERDEF
class. the loader function is called with the class itself,
instead of an allocated object, and the loaded data.

* marshal.c (compat_allocator_table): initialize
compat_allocator_tbl on demand.

* object.c (rb_undefined_alloc): extract from rb_obj_alloc.

* marshal.c (compat_allocator_table): initialize

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52974 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision bd4364ac - 12/08/2015 04:44 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52856,52906: [Backport #11760]

* encoding.c (enc_m_loader): defer finding encoding object not to
be infected by marshal source. [ruby-core:71793] [Bug #11760]

* marshal.c (r_object0): enable compatible loader on USERDEF
class. the loader function is called with the class itself,
instead of an allocated object, and the loaded data.

* marshal.c (compat_allocator_table): initialize
compat_allocator_tbl on demand.

* object.c (rb_undefined_alloc): extract from rb_obj_alloc.

* marshal.c (compat_allocator_table): initialize

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52974 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 12/02/2015 07:27 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset r52856.

encoding.c: defer finding encoding

- encoding.c (enc_m_loader): defer finding encoding object not to be infected by marshal source. [\[ruby-core:71793\]](#) [Bug [#11760](#)]
- marshal.c (r_object0): enable compatible loader on USERDEF class. the loader function is called with the class itself, instead of an allocated object, and the loaded data.
- marshal.c (compat_allocator_table): initialize compat_allocator_tbl on demand.
- object.c (rb_undefined_alloc): extract from rb_obj_alloc.

#2 - 12/08/2015 02:51 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED

ruby_2_1 r52933 merged revision(s) 52856,52906.

#3 - 12/08/2015 04:45 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

Backported into ruby_2_2 branch at r52974.