Ruby master - Bug #10988

[PATCH] Raise ArgumentError when string passed to String#crypt contains null

03/20/2015 01:35 PM - jrusnack (Jan Rusnacko)

<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>2.3.0dev</td>
</tr>
<tr>
<td>ruby -v:</td>
<td>2.3.0dev</td>
</tr>
<tr>
<td>Backport:</td>
<td>2.0.0: WONTFIX, 2.1: WONTFIX, 2.2: WONTFIX</td>
</tr>
</tbody>
</table>

Description

Currently String#crypt assumes that it is called on a password typed by the user, specifically, that it does not contain null character. When it does:

```
"abc\0def".crypt("pass") == "abc".crypt("pass")
=> true
```

This may not be desirable, and developers invoking crypt on strings that potentially include null may expect different results. To prevent security failures, this patch changes String#crypt to throw ArgumentError when invoked on String that includes null character.

https://www.reddit.com/r/netsec/comments/2yugos/null_bytes_bcrypt_problem/

Also PR: https://github.com/ruby/ruby/pull/853

Associated revisions

Revision f64ac5d4 - 05/10/2015 02:49 AM - glass

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null.
  the patch is from jrusnack .
  [Bug #10988] [fix GH-853]

- test/ruby/test_string.rb: test for above.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@50458 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 50458 - 05/10/2015 02:49 AM - Glass_saga (Masaki Matsushita)

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null.
  the patch is from jrusnack .
  [Bug #10988] [fix GH-853]

- test/ruby/test_string.rb: test for above.

Revision 50458 - 05/10/2015 02:49 AM - glass

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null.
  the patch is from jrusnack .
  [Bug #10988] [fix GH-853]
Revision 50458 - 05/10/2015 02:49 AM - glass

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null. the patch is from jrusnack.
  [Bug #10988] [fix GH-853]

- test/ruby/test_string.rb: test for above.

Revision 50458 - 05/10/2015 02:49 AM - glass

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null. the patch is from jrusnack.
  [Bug #10988] [fix GH-853]

- test/ruby/test_string.rb: test for above.

Revision 50458 - 05/10/2015 02:49 AM - glass

- string.c (rb_str_crypt): Raise ArgumentError when string passed to String#crypt contains null. the patch is from jrusnack.
  [Bug #10988] [fix GH-853]

- test/ruby/test_string.rb: test for above.

History

#1 - 03/21/2015 06:21 AM - nobu (Nobuyoshi Nakada)
I agree this behavior would be better, but maybe a feature request?

#2 - 05/10/2015 02:49 AM - Anonymous
- Status changed from Open to Closed

Applied in changeset r50458.

#3 - 06/30/2015 04:19 AM - usa (Usaku NAKAMURA)
- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: WONTFIX, 2.1: WONTFIX, 2.2: UNKNOWN

#4 - 07/02/2015 04:54 AM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 2.0.0: WONTFIX, 2.1: WONTFIX, 2.2: UNKNOWN to 2.0.0: WONTFIX, 2.1: WONTFIX, 2.2: WONTFIX
<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-Raise-ArgumentError-when-string-passed-to-String-cry.patch</td>
<td>1.87 KB</td>
<td>03/20/2015</td>
<td>jrusnack (Jan Rusnacko)</td>
</tr>
</tbody>
</table>