Ruby master - Bug #13376

Symbol#hash is deterministic on 2.3

03/28/2017 04:00 PM - chrisseaton (Chris Seaton)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.3.3p222 (2016-11-21 revision 56859) [x86_64-darwin16]	**Backport:**	2.2: DONTNEED, 2.3: DONE, 2.4: UNKNOWN

Description

I believe the Symbol#hash should probably be non-deterministic, due to CVE-2011-4815. That seems to be the behaviour on 2.2 and 2.4, but not on 2.3. Was this a conscious decision at the time? Or is it a bug?

```
$ 2.2.6/bin/ruby -e 'puts :foo.hash'
-505215953858886063

$ 2.2.6/bin/ruby -e 'puts :foo.hash'
3929535091178311289

$ 2.3.3/bin/ruby -e 'puts :foo.hash'
2810

$ 2.3.3/bin/ruby -e 'puts :foo.hash'
2810

$ 2.4.0/bin/ruby -e 'puts :foo.hash'
-1200094397129038718

$ 2.4.0/bin/ruby -e 'puts :foo.hash'
-916960310565036298
```

Associated revisions

Revision 149d43d4 - 03/28/2017 05:14 PM - normal

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks. This is currently the
case since 2.4+, but was not for the 2.3 series.

- test/ruby/test_symbol.rb (test_hash_nondeterministic): new test [ruby-core:80430] [Bug #13376]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@58200 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 58200 - 03/28/2017 05:14 PM - normalperson (Eric Wong)

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks. This is currently the
case since 2.4+, but was not for the 2.3 series.

- test/ruby/test_symbol.rb (test_hash_nondeterministic): new test [ruby-core:80430] [Bug #13376]

Revision 58200 - 03/28/2017 05:14 PM - normal

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks. This is currently the
case since 2.4+, but was not for the 2.3 series.

- test/ruby/test_symbol.rb (test_hash_nondeterministic): new test [ruby-core:80430] [Bug #13376]

Revision 58200 - 03/28/2017 05:14 PM - normal

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks. This is currently the
case since 2.4+, but was not for the 2.3 series.

- test/ruby/test_symbol.rb (test_hash_nondeterministic): new test [ruby-core:80430] [Bug #13376]

Revision 4634c34d - 03/28/2017 09:29 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 58200: [Backport #13376]

```
    * hash.c (any_hash): fix Symbol#hash to be nondeterministic.
      The patch was provided by Eric Wong. [ruby-core:80433] [Bug #13376]

    test/ruby/test_symbol.rb: new test for nondeterminism

    We need to ensure hashes for static symbols remain
    non-deterministic to avoid DoS attacks.   This is currently the
    case since 2.4+, but was not for the 2.3 series.

    * test/ruby/test_symbol.rb (test_hash_nondeterministic): new test
      [ruby-core:80430] [Bug #13376]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@58203 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 58203 - 03/28/2017 09:29 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 58200: [Backport #13376]

```
* hash.c (any_hash): fix Symbol#hash to be nondeterministic.
  The patch was provided by Eric Wong. [ruby-core:80433] [Bug #13376]

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks.   This is currently the
case since 2.4+, but was not for the 2.3 series.

* test/ruby/test_symbol.rb (test_hash_nondeterministic): new test
  [ruby-core:80430] [Bug #13376]
```

Revision 0ad16855 - 03/29/2017 03:00 PM - nagachika (Tomoyuki Chikanaga)

- hash.c (any_hash): fix CI failure on L32LLP64 architecture. The patch was provided by usa. [ruby-core:80484] [Bug #13376]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@58213 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 58213 - 03/29/2017 03:00 PM - nagachika (Tomoyuki Chikanaga)

- hash.c (any_hash): fix CI failure on L32LLP64 architecture. The patch was provided by usa. [ruby-core:80484] [Bug #13376]

History

#1 - 03/28/2017 04:36 PM - normalperson (Eric Wong)

chris@chrisseaton.com wrote:

> Bug #13376: Symbol#hash is deterministic on 2.3
> https://bugs.ruby-lang.org/issues/13376

I think I broke this in:

commit 14470aa6dbf4d99bc8e0484e1334c2c6d5e68fc3 / r51582
("hash.c: improve integer/fixnum hashing")

and nobu fixed this in:

commit a49f6016ea48a40865c91137b33ff9115e4071fd / r56992
("switching hash removal")

Which was too big to backport... I will come up with a 2.3-only fix.

#2 - 03/28/2017 05:00 PM - normalperson (Eric Wong)

- Backport changed from 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: UNKNOWN

- File 0001-hash.c-any_hash-make-static-symbol-hash-non-determin.patch added

Here is a 2.3-only patch.

#3 - 03/28/2017 05:14 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset trunk|r58200.

---

test/ruby/test_symbol.rb: new test for nondeterminism

We need to ensure hashes for static symbols remain
non-deterministic to avoid DoS attacks. This is currently the
case since 2.4+, but was not for the 2.3 series.

- test/ruby/test_symbol.rb (test_hash_nondeterministic): new test [ruby-core:80430] [Bug #13376]

#4 - 03/28/2017 05:22 PM - normalperson (Eric Wong)

I also committed r58200 to trunk to prevent us from hitting
this, again. We should ensure other classes don't suffer this
fate, too, will check other cases later (or if other people send
patches).

/me goes back to hibernation

#5 - 03/28/2017 06:02 PM - Eregon (Benoit Daloze)

For information, https://github.com/ruby/spec/pull/393 is adding such tests in ruby/spec
for Object, Integer, Float, String, Symbol, Array and Hash.
That's how the bug was discovered.

#6 - 03/28/2017 09:31 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: DONE, 2.4: UNKNOWN

Thank you Chris for your report. And thank you Eric creating a patch for ruby_2_3!

I backported r58200 with Eric's patch into ruby_2_3 branch at r58203.

#7 - 03/29/2017 02:09 PM - darix (Marcus Rückert)

should this receive a new CVE?
should this released be soon as 2.3.4?

#8 - 03/29/2017 02:21 PM - nobu (Nobuyoshi Nakada)

Accepting huge requests which could exhaust memory with too may symbols *at once* would be rarely possible in 2.3.

#9 - 03/29/2017 02:27 PM - Eregon (Benoit Daloze)

nobu (Nobuyoshi Nakada) wrote:

> Accepting huge requests which could exhaust memory with too may symbols *at once* would be rarely possible in 2.3.

CVE-2011-4815 is about hash collisions, which indeed seems possible if a user can control Symbol keys inserted into a Hash in 2.3.

#10 - 03/29/2017 02:35 PM - usa (Usaku NAKAMURA)

I've fixed it.
nagachika-san, please apply this patch:

```
Index: hash.c
===================================================================
--- hash.c  (revision 58210)
```

```
+++ hash.c  (working copy)
@@ -168,7 +168,7 @@ any_hash(VALUE a, st_index_t (*other_func)(VALUE))
     }
   out:
     hnum <<= 1;
-    return (st_index_t)RSHIFT(hnum, 1);
+    return (long)RSHIFT(hnum, 1);
 }

 static st_index_t
```

#11 - 03/29/2017 02:59 PM - nagachika (Tomoyuki Chikanaga)

Thank you usa-san. I'll merge your patch soon.
I'd like to make v2_3_4 tag after confirming the result of CI on vc12-x64.

#12 - 04/30/2017 12:12 PM - usa (Usaku NAKAMURA)

- Backport changed from 2.2: UNKNOWN, 2.3: DONE, 2.4: UNKNOWN to 2.2: DONTNEED, 2.3: DONE, 2.4: UNKNOWN

Files

0001-hash.c-any_hash-make-static-symbol-hash-non-determin.patch	1.7 KB	03/28/2017	normalperson (Eric Wong)