# Ruby master - Bug #15335

## Ruby 2.6.0 is not properly fortified

11/23/2018 08:48 AM - vo.x (Vit Ondruch)

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | ioquatix (Samuel Williams) | | |
| **Target version:** | | | |
| **ruby -v:** | ruby 2.6.0dev (2018-11-22 trunk 65928) [x86_64-linux] | **Backport:** | 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN |

**Description**

For some while, we carry this test in Fedora package 1:

```
checksec -f libruby.so.%{ruby_version} | \
  grep "Full RELRO.*Canary found.*NX enabled.*DSO.*No RPATH.*No RUNPATH.*Yes.*\d*.*\d*.*libruby.so
.%{ruby_version}"
```

This should ensure, that the library is properly fortified 2. This test was passing with preview3, but it started to fail, testing with r65928:

```
$ checksec -f libruby.so.2.6.0
WARNING: 'openssl' not found! It's required for most checks.

WARNING: Not all necessary commands found. Some tests might not work!

RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH  FORTIFY Fortif
ied Fortifiable  FILE
Full RELRO      Canary found      NX disabled   DSO             No RPATH   No RUNPATH   Yes 16
  42  libruby.so.2.6.0
```

The NX disabled is the difference. Looking at the log, it is definitely not about configuration options. So if I should point finger at something, it seems to me that this must be it:

```
... snip ...

assembling coroutine/amd64/Context.s
gcc -I. -I.ext/include/x86_64-linux -I./include -I. -I./enc/unicode/10.0.0 -o coroutine/amd64/Cont
ext.o -c coroutine/amd64/Context.s

... snip ...

gcc -shared -Wl,-z,relro -Wl,--as-needed  -Wl,-z,now -specs=/usr/lib/rpm/redhat/redhat-hardened-ld
 -Wl,-soname,libruby.so.2.6 -fstack-protector-strong  -m64 dln.o localeinit.o loadpath.o array.o a
st.o bignum.o class.o compar.o compile.o complex.o cont.o debug.o debug_counter.o dir.o dln_find.o
 encoding.o enum.o enumerator.o error.o eval.o file.o gc.o hash.o inits.o io.o iseq.o load.o marsh
al.o math.o mjit.o mjit_compile.o node.o numeric.o object.o pack.o parse.o proc.o process.o random
.o range.o rational.o re.o regcomp.o regenc.o regerror.o regexec.o regparse.o regsyntax.o ruby.o s
afe.o signal.o sprintf.o st.o strftime.o string.o struct.o symbol.o thread.o time.o transcode.o tr
ansient_heap.o util.o variable.o version.o vm.o vm_backtrace.o vm_dump.o vm_trace.o coroutine/amd6
4/Context.o probes.o enc/ascii.o enc/us_ascii.o enc/unicode.o enc/utf_8.o enc/trans/newline.o setp
roctitle.o strlcat.o strlcpy.o addr2line.o  prelude.o dmyext.o dmyenc.o -lpthread -lrt -lrt -lgmp
-ldl -lcrypt -lm   -o libruby.so.2.6.0

... snip ...
```

I.e. the coroutines assembly. Not sure how to prove it nor fix it.

**Related issues:**

| | |
|---|---|
| Related to Ruby master - Bug #16762: Ruby is not properly fortified on armv7hl | **Open** |

**Associated revisions**

**Revision dc6908ab - 12/11/2018 11:49 PM - samuel**

Ensure x86 stack is fortified, fixed #15335.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@66341 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 66341 - 12/11/2018 11:49 PM - samuel**

Ensure x86 stack is fortified, fixed #15335.

**Revision 66341 - 12/11/2018 11:49 PM - samuel**

Ensure x86 stack is fortified, fixed #15335.

## History

**#1 - 11/24/2018 07:18 AM - mame (Yusuke Endoh)**

*- Assignee set to ioquatix (Samuel Williams)*

*- Status changed from Open to Assigned*

**#2 - 11/24/2018 07:30 AM - ioquatix (Samuel Williams)**

How can we solve this problem?

**#3 - 11/24/2018 07:52 AM - normalperson (Eric Wong)**

> https://bugs.ruby-lang.org/issues/15335#change-75132

samuel@oriontransfer.net wrote:

> How can we solve this problem?

Fedora can configure with --disable-fiber-coroutine option
as a stopgap...

> I.e. the coroutines assembly. Not sure how to prove it nor fix it.

Maybe this can help?
https://wiki.gentoo.org/wiki/Hardened/GNU_stack_quickstart

**#4 - 11/24/2018 09:19 AM - ioquatix (Samuel Williams)**

Thanks Eric. Those two suggestions are really helpful. I'll investigate it now.

**#5 - 11/24/2018 11:12 AM - ioquatix (Samuel Williams)**

I'm attempting to fix this issue here: https://github.com/ruby/ruby/pull/2027

vo.x (Vit Ondruch) do you mind trying to build that PR?

**#6 - 11/24/2018 11:35 AM - ioquatix (Samuel Williams)**

I've merged the first set of changes into trunk, for amd64 - vo.x (Vit Ondruch) if you confirm this has fixed the issue I will extend to other architectures.

**#7 - 11/24/2018 03:58 PM - vo.x (Vit Ondruch)**

Thx. I hope I'll be able to check it on Monday.

**#8 - 11/26/2018 11:38 AM - vo.x (Vit Ondruch)**

Testing with r65990 on x86_64 and the test passed. I guess I should not try to build on other arches yet, right?

**#9 - 11/29/2018 02:47 PM - vo.x (Vit Ondruch)**

Just FTR trying to build r66092 on Fedora Rawhide 1, x86_64, ppc64le, aarch64, s390x, and armv7hl were properly fortified while only i686 failed to pass 2 the fortification test.

**#10 - 12/11/2018 11:49 PM - Anonymous**

*- Status changed from Assigned to Closed*

Applied in changeset trunk|r66341.

---

Ensure x86 stack is fortified, fixed #15335.

#### #11 - 12/12/2018 12:00 AM - ioquatix (Samuel Williams)

I've fixed x86 implementation too, now that it was confirmed the previous effort to fix x64 worked as expected. This issue should be completely resolved now (dc6908ab44c3a3fc78319422410b57d3b7fb6c0c / r66341).

#### #12 - 01/04/2019 02:09 PM - vo.x (Vit Ondruch)

ioquatix (Samuel Williams) wrote:

> I've fixed x86 implementation too.

Thx, I can build Ruby 2.6.0 on all platforms just fine.

#### #13 - 04/06/2020 05:13 PM - vo.x (Vit Ondruch)

*- Related to Bug #16762: Ruby is not properly fortified on armv7hl added*