

Ruby trunk - Bug #10019

segmentation fault/buffer overrun in pack.c (encodes)

07/09/2014 02:40 PM - wkwood (Will Wood)

Status:	Feedback	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.1.2p168 (2014-07-06 revision 46721) [i386-mingw32]	Backport: 2.0.0: REQUIRED, 2.1: DONE

Description

While working with an AWS sample I hit a segmentation fault. The same sample works under 1.9.3. It appeared to be coming from pack.c function encodes. After looking at the source there's a 4K buffer allocated on the stack. I made a minor change to base the buffer length off of the incoming buffer length with a pad and allocate it off the heap. Anyway, after fixing this my code sample runs fine. I'm including a patch file and the sample code.

Associated revisions

Revision 8a608d2b - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@46778 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 46778 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]

Revision 5c1a6945 - 07/13/2014 01:59 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r46778: [Backport #10019]

```
* pack.c (encodes): fix buffer overrun by tail_lf. Thanks to
Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]
```

Revision 46806 - 07/13/2014 01:59 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r46778: [Backport #10019]

```
* pack.c (encodes): fix buffer overrun by tail_lf. Thanks to
  Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug #10019]
```

History

#1 - 07/09/2014 05:06 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Feedback
- Priority changed from Normal to 3

encodes() fills and flush buff gradually by the buffer size.
Could you show the message at the segmentation fault?

Anyway, your patch includes unnecessary garbage.

#2 - 07/10/2014 09:24 AM - mtasaka (Mamoru Tasaka)

Looking at encodes(), it seems at least when

- len = 3070 (= ((4096 - 4) / 4 * 3 + 1))
- tail_lf = 1 encodes() causes segv at <https://github.com/ruby/ruby/blob/trunk/pack.c#L987>

#3 - 07/10/2014 09:28 AM - mtasaka (Mamoru Tasaka)

... and type is not 'u'.

#4 - 07/10/2014 01:23 PM - nobu (Nobuyoshi Nakada)

But if tail_lf is 1, len is a multiple of 3, so it can't be 3070.

#5 - 07/10/2014 01:32 PM - nobu (Nobuyoshi Nakada)

Am I missing something?

#6 - 07/10/2014 06:22 PM - thoger (Tomas Hoger)

Nobuyoshi Nakada wrote:

But if tail_lf is 1, len is a multiple of 3, so it can't be 3070.

len in encodes() can be anything between 1 and len from pack_pack() (which is a multiple of 3). It is possible to trigger mentioned off-by-one overflow one of the following ways:

- the length of the input string is 3070 (or 3071) and count value for the m format directive is 3072 or more
- count value for the m format directive is exactly 3072 and the length of the input string is n*3072 - 2 (or -1)

I.e.:

- ["a"*3070].pack("m4000")
- ["a"*(3072*3-2)].pack("m3072")

Depending on platform, compiler, compiler flags, ... this may or may not produce reliable crash.

Anyway, it's unclear if that is the problem observed by reporter. The aws-sdk and its dependencies only seem to use pack("m0"), which can not trigger this overflow.

#7 - 07/11/2014 01:09 AM - nobu (Nobuyoshi Nakada)

- Status changed from Feedback to Closed
- % Done changed from 0 to 100

Applied in changeset r46778.

pack.c: fix buffer overrun

- pack.c (encodes): fix buffer overrun by tail_lf. Thanks to Mamoru Tasaka and Tomas Hoger. [ruby-core:63604] [Bug [#10019](#)]

#8 - 07/11/2014 01:57 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN to 2.0.0: REQUIRED, 2.1: REQUIRED

#9 - 07/13/2014 01:59 PM - nagachika (Tomoyuki Chikanaga)

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

Backported into ruby_2_1 branch at r46806.

#10 - 07/15/2014 02:52 PM - rcvalle (Ramon de C Valle)

It seems that the (off-by-one) issue is also present in Ruby 1.9.3, requiring a backport too.

It may also worth confirming with the reporter if he continues to observe the crash after adding the fix, since as Tomas analysis of aws-sdk gem and its dependencies indicates it's unlikely this issue is being caused by any of these gems. So, it may be the case the reporter may be referring to a different issue.

#11 - 07/19/2014 04:33 PM - wkwood (Will Wood)

After pulling the latest code, your fix still causes a seg fault. IMO you're still overrunning the buffer.

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38: [BUG] Segmentation fault
ruby 2.1.2p176 (2014-07-19 revision 46869) [i386-mingw32]
```

```
-- Control frame information -----
c:0027 p:---- s:0143 e:000142 CFUNC :pack
c:0026 p:0012 s:0139 e:000138 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38
c:0025 p:0026 s:0135 e:000134 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/signers/base.rb:
c:0024 p:0042 s:0129 e:000128 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/signers/s3.rb:59
c:0023 p:0019 s:0123 e:000119 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/signers/s3.rb:53
c:0022 p:0041 s:0116 e:000112 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/signers/s3.rb:47
c:0021 p:0100 s:0108 e:000107 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/s3/client.rb:59
c:0020 p:0028 s:0103 e:000102 BLOCK d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:492 [F
c:0019 p:---- s:0100 e:000099 CFUNC :call
c:0018 p:0009 s:0097 e:000096 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/response.rb:175
c:0017 p:0066 s:0094 e:000093 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/response.rb:114
c:0016 p:---- s:0088 e:000087 CFUNC :new
c:0015 p:0017 s:0085 e:000084 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:203
c:0014 p:0063 s:0079 E:0026bc BLOCK d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:490
c:0013 p:0019 s:0073 e:000072 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:391
c:0012 p:0009 s:0066 E:000e6c BLOCK d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:477
c:0011 p:0006 s:0064 e:000063 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:373
c:0010 p:0009 s:0058 E:001308 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/client.rb:476
c:0009 p:0031 s:0052 e:000051 METHOD (eval):3
c:0008 p:0011 s:0046 e:000045 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/s3/object_collection.
c:0007 p:0061 s:0042 e:000041 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/s3/paginated_collecti
c:0006 p:0126 s:0034 E:0022dc METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/collection/with_
c:0005 p:0017 s:0023 e:000022 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/collection.rb:80
c:0004 p:0013 s:0018 E:000f04 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/core/collection.rb:47
c:0003 p:0014 s:0013 e:000012 METHOD d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aw
s/s3/object_collection.
c:0002 p:0083 s:0008 E:001f5c EVAL BucketCleaner.rb:13 [FINISH]
c:0001 p:0000 s:0002 E:0011c4 TOP [FINISH]
```

```
BucketCleaner.rb:13:in `<main>'
```

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/object_collection.rb:282:in `each'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/collection.rb:47:in `each'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/collection.rb:80:in `each_batch'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/collection/with_limit_and_next_token.rb:54:in `_each'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/paginated_collection.rb:29:in `_each_item'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/object_collection.rb:295:in `list_request'
(eval):3:in `list_objects'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:476:in `client_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:373:in `return_or_raise'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:477:in `block in client_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:391:in `log_client_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:490:in `block (2 levels) in client_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:203:in `new_response'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:203:in `new'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/response.rb:114:in `initialize'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/response.rb:175:in `build_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/response.rb:175:in `call'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb:492:in `block (3 levels) in client_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/client.rb:59:in `sign_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/s3.rb:47:in `sign_request'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/s3.rb:53:in `authorization'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/s3.rb:59:in `signature'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/base.rb:29:in `sign'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38:in `encode64'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38:in `pack'
```

-- C level backtrace information -----

```
C:\windows\SYSTEM32\ntdll.dll(NtWaitForSingleObject+0xc) [0x770ccd7c]
C:\windows\SYSTEM32\KERNELBASE.dll(WaitForSingleObject+0x12) [0x74f1103d]
d:\ruby-2.1.2-i386-mingw32\bin\msvcrt-ruby210.dll(rb_vm_bugreport+0xf5) [0x6d3ade25]
d:\ruby-2.1.2-i386-mingw32\bin\msvcrt-ruby210.dll(rb_name_err_msg_new+0x1de) [0x6d24eb3e]
d:\ruby-2.1.2-i386-mingw32\bin\msvcrt-ruby210.dll(rb_bug+0x2f) [0x6d24f8af]
d:\ruby-2.1.2-i386-mingw32\bin\msvcrt-ruby210.dll(rb_check_safe_str+0x170) [0x6d323fb0]
[0x004011e6]
C:\windows\SYSTEM32\KERNELBASE.dll(UnhandledExceptionFilter+0x142) [0x74fc966d]
C:\windows\SYSTEM32\ntdll.dll(LdrSetAppCompatDllRedirectionCallback+0x187b5) [0x77133894]
```

-- Other runtime information -----

* Loaded script: BucketCleaner.rb

* Loaded features:

- 0 enumerator.so
- 1 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/encdb.so
- 2 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/iso_8859_1.so
- 3 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/trans/transdb.so
- 4 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/rbconfig.rb
- 5 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/compatibility.rb
- 6 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/defaults.rb
- 7 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/deprecate.rb
- 8 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/errors.rb
- 9 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/version.rb
- 10 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/requirement.rb
- 11 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/platform.rb
- 12 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/basic_specification.rb
- 13 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/stub_specification.rb
- 14 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/util/stringio.rb

15 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/specification.rb
16 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/exceptions.rb
17 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/defaults/operating_system.rb
18 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/core_ext/kernel_gem.rb
19 thread.rb
20 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/thread.so
21 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/monitor.rb
22 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/core_ext/kernel_require.rb
23 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems.rb
24 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/path_support.rb
25 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rubygems/dependency.rb
26 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/set.rb
27 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/digest.so
28 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/digest.rb
29 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/openssl.so
30 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/bn.rb
31 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/cipher.rb
32 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/stringio.so
33 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/config.rb
34 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/digest.rb
35 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/x509.rb
36 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/buffering.rb
37 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/fcntl.so
38 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl/ssl.rb
39 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/openssl.rb
40 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/securerandom.rb
41 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/common.rb
42 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/generic.rb
43 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/ftp.rb
44 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/http.rb
45 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/https.rb
46 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/ldap.rb
47 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/ldaps.rb
48 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri/mailto.rb
49 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/uri.rb
50 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/socket.so
51 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/socket.rb
52 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/timeout.rb
53 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/protocol.rb
54 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/zlib.so
55 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/exceptions.rb
56 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/header.rb
57 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/generic_request.rb
58 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/request.rb
59 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/requests.rb
60 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/response.rb
61 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/responses.rb
62 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/proxy_delta.rb
63 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http/backward.rb
64 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/http.rb
65 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/net/https.rb
66 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/logger.rb
67 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/http/connection_pool.rb
68 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/pathname.so
69 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/pathname.rb
70 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/log_formatter.rb
71 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/configuration.rb
72 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/cloud_front/config.rb
73 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/cloud_search/config.rb
74 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/cloud_trail/config.rb
75 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/cloud_watch/config.rb
76 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/dynamo_db/config.rb
77 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/ec2/config.rb
78 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/emr/config.rb
79 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/elasticache/config.rb
80 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/glacier/config.rb
81 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/rds/config.rb
82 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/route_53/config.rb
83 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/simple_email_service/config.r
b
84 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/sns/config.rb
85 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/sqs/config.rb
86 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/simple_workflow/config.rb
87 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/simple_db/config.rb
88 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/auto_scaling/config.rb

89 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/cloud_formation/config.rb
90 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/data_pipeline/config.rb
91 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/direct_connect/config.rb
92 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/elastic_beanstalk/config.rb
93 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/iam/config.rb
94 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/import_export/config.rb
95 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/kinesis/config.rb
96 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/ops_works/config.rb
97 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/sts/config.rb
98 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/storage_gateway/config.rb
99 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/support/config.rb
100 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/elb/config.rb
101 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/elastic_transcoder/config.rb
102 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/redshift/config.rb
103 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/config.rb
104 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core.rb
105 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/exception.rb
106 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/syntax_error.rb
107 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/psych.so
108 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/omap.rb
109 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/set.rb
110 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/class_loader.rb
111 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/strscan.so
112 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/scalar_scanner.rb
113 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/node.rb
114 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/stream.rb
115 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/document.rb
116 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/sequence.rb
117 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/scalar.rb
118 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/mapping.rb
119 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes/alias.rb
120 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/nodes.rb
121 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/streaming.rb
122 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/visitor.rb
123 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/to_ruby.rb
124 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/emitter.rb
125 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/handler.rb
126 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/tree_builder.rb
127 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/yaml_tree.rb
128 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/json/ruby_events.rb
129 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/json_tree.rb
130 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors/depth_first.rb
131 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/visitors.rb
132 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/parser.rb
133 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/coder.rb
134 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/core_ext.rb
135 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/date_core.so
136 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/date/format.rb
137 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/date.rb
138 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/deprecated.rb
139 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/stream.rb
140 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/json/yaml_events.rb
141 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/json/tree_builder.rb
142 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/json/stream.rb
143 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych/handlers/document_stream.rb
144 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/psych.rb
145 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/yaml.rb
146 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/rails.rb
147 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws-sdk.rb
148 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/service_interface.rb
149 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/xml/grammar.rb
150 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/lazy_error_classes.rb
151 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/meta_utils.rb
152 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/errors.rb
153 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/errors.rb
154 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3.rb
155 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/inflection.rb
156 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/json/version.rb
157 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/ostruct.rb
158 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/json/generic_object.rb
159 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/json/common.rb
160 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/utf_16be.so
161 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/utf_16le.so
162 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/utf_32be.so
163 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/enc/utf_32le.so

164 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/json/ext/parser.so
165 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/json/ext/generator.so
166 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/json/ext.rb
167 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/json.rb
168 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/endpoints.rb
169 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/time.rb
170 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/credential_providers.rb
171 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/http/net_http_handler.rb
172 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/security.rb
173 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parseexception.rb
174 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/formatters/default.rb
175 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/formatters/pretty.rb
176 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/node.rb
177 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/child.rb
178 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parent.rb
179 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/xmltokens.rb
180 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/namespace.rb
181 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/encoding.rb
182 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/source.rb
183 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/entity.rb
184 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/attlistdecl.rb
185 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/doctype.rb
186 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/text.rb
187 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/attribute.rb
188 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/cdata.rb
189 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/functions.rb
190 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/syncenumerator.rb
191 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parsers/xpathparser.rb
192 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/xpath_parser.rb
193 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/xpath.rb
194 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/element.rb
195 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/xmldecl.rb
196 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/comment.rb
197 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/instruction.rb
198 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/rexml.rb
199 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/output.rb
200 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/undefinednamespaceexception.rb
201 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parsers/baseparser.rb
202 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parsers/streamparser.rb
203 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/validation/validationexception.rb
204 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/parsers/treeparser.rb
205 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/rexml/document.rb
206 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/digest/md5.so
207 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb
208 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/2.1/noko
giri.so
209 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/version.
rb
210 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/syntax_e
rror.rb
211 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/pp/n
ode.rb
212 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/pp/c
haracter_data.rb
213 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/pp.r
b
214 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/pars
e_options.rb
215 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/sax/
document.rb
216 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/sax/
parser_context.rb
217 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/sax/
parser.rb
218 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/sax/
push_parser.rb
219 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/sax.
rb
220 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/node
/save_options.rb
221 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/node
.rb
222 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/attr
ibute_decl.rb
223 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/elem

ent_decl.rb
224 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/element_content.rb
225 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/character_data.rb
226 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/namespacespace.rb
227 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/attribute.rb
228 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/dtd.rb
229 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/cdata.rb
230 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/text.rb
231 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/document.rb
232 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/document_fragment.rb
233 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/processing_instruction.rb
234 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/node_set.rb
235 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/syntax_error.rb
236 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/xpath/syntax_error.rb
237 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/xpath.rb
238 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/xpath/context.rb
239 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/builder.rb
240 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/reader.rb
241 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/notation.rb
242 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/entity_decl.rb
243 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/schema.rb
244 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml/relax_ng.rb
245 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xml.rb
246 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xslt/stylesheet.rb
247 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/xslt.rb
248 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/entity_lookup.rb
249 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/document.rb
250 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/document_fragment.rb
251 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/sax/parser_context.rb
252 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/sax/parser.rb
253 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/sax/push_parser.rb
254 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/element_description.rb
255 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/element_description_default.rb
256 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html.rb
257 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/decorators/slop.rb
258 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/node.rb
259 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/xpath_visitor.rb
260 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/i386-mingw32/racc/cparse.so
261 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/racc/parser.rb
262 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/parser_extras.rb
263 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/parser


```
er.rb
 264 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/toke
nizer.rb
 265 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css/synt
ax_error.rb
 266 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/css.rb
 267 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri/html/bui
lder.rb
 268 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/nokogiri-1.6.3.rc3-x86-mingw32/lib/nokogiri.rb
 269 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/deprecations.rb
 270 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/naming.rb
 271 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/client.rb
 272 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/data_options.rb
 273 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/cgi/core.rb
 274 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/cgi/util.rb
 275 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/cgi/cookie.rb
 276 d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/cgi.rb
 277 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/uri_escape.rb
 278 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/client/xml.rb
 279 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/xml/parser.rb
 280 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/client.rb
 281 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/model.rb
 282 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/bucket_collection.rb
 283 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/acl_options.rb
 284 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/bucket.rb
 285 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/collection.rb
 286 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/collection/with_limit_an
d_next_token.rb
 287 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/paginated_collection.rb
 288 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/prefixed_collection.rb
 289 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/prefix_and_delimiter_colle
ction.rb
 290 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/object_collection.rb
 291 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/async_handle.rb
 292 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/response.rb
 293 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/http/request.rb
 294 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/s3/request.rb
 295 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/version.rb
 296 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/s3.rb
 297 d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/base.rb
```

[NOTE]

You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: <http://www.ruby-lang.org/bugreport.html>

This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.

#12 - 07/19/2014 11:48 PM - nobu (Nobuyoshi Nakada)

- Status changed from Closed to Feedback

- Priority changed from 3 to Normal

Will Wood wrote:

After pulling the latest code, your fix still causes a seg fault. IMO you're still overrunning the buffer.

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/base.rb:29:in `sig
n'
d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38:in `encode64'
```

Can't you show the argument to encode64?

#13 - 07/21/2014 08:36 AM - thoger (Tomas Hoger)

Will Wood wrote:

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/s3.rb:59:in `signature'
```

<https://github.com/aws/aws-sdk-ruby/blob/e243394/lib/aws/core/signers/s3.rb#L59>

```
signature = Base.sign(credentials.secret_access_key, signature, 'sha1')
```

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/gems/2.1.0/gems/aws-sdk-1.48.1/lib/aws/core/signers/base.rb:29:in `sign'
```

<https://github.com/aws/aws-sdk-ruby/blob/2feef15/lib/aws/core/signers/base.rb#L29>

```
Base64.encode64(hmac(secret, string_to_sign, digest_method)).strip
```

where hmac() is:

<https://github.com/aws/aws-sdk-ruby/blob/2feef15/lib/aws/core/signers/base.rb#L38>

```
def hmac key, value, digest = 'sha256'  
  OpenSSL::HMAC.digest(OpenSSL::Digest.new(digest), key, value)  
end
```

```
d:/ruby-2.1.2-i386-mingw32/lib/ruby/2.1.0/base64.rb:38:in `encode64'
```

http://svn.ruby-lang.org/cgi-bin/viewvc.cgi/branches/ruby_2_1/lib/base64.rb?revision=44340&view=markup#l38

```
[bin].pack("m")
```

Value passed to encode64() should be short, and of fixed size for a given digest method. For SHA-1, that's 20 bytes, hence output size is 28+1 bytes. That should be far from overflowing buff[4096].

Hence the minimal reproducer should be:

```
require 'openssl'  
digest = OpenSSL::Digest.new('sha1')  
hmac_val = OpenSSL::HMAC.digest(digest, 'secret', 'value')  
print [hmac_val].pack('m')
```

As encode64() output size only depend on input size, and not input content, it should not matter what 'secret' and 'value' are.

#14 - 07/23/2014 01:25 AM - wkwood (Will Wood)

I agree the argument should be short. I'm working on it, but it's definitely strange. If I take the buffer and allocate it off the heap it's fine. Maybe it's a build issue with RubyInstaller? Anyway, I'll poke around with and get back with you in a day or two.

#15 - 07/28/2014 02:50 PM - wkwood (Will Wood)

- File pack.c.patch added

I took a look at it yesterday. Here's the issue. In the loop (len >= 3) you check to see if there's enough room in buff. Unfortunately if len < 3 we don't flush the buffer and then write additional bytes onto the end without checking. I added a check to flush the buffer if len < 3 and then there's enough space on exiting the loop for the remaining bytes and padding including lf. The patch attached fixes the problem. You also don't need the + 1 byte or a 4K buffer either, your call but patch is 256 bytes for the buffer. I don't like large objects on the heap, that's just me. No seg faults for me and it works with this patch just fine. Also the rb_bug test at the end isn't necessary, your call if you want to remove it but it'll never get executed.

#16 - 07/28/2014 03:42 PM - thoger (Tomas Hoger)

Will Wood wrote:

Here's the issue. In the loop (len >= 3) you check to see if there's enough room in buff. Unfortunately if len < 3 we don't flush the buffer and then write additional bytes onto the end without checking.

The check at the end of each iteration of the while loop ensures that there are at least 4 bytes left in the buff. So there is enough space to write additional 4 output bytes for the remaining 1 or 2 input bytes with padding if 0 < len < 3. Only the additional '\n' written in the tail_if == 1 case was not accounted for, and was addressed by the +1.

You also don't need the + 1 byte or a 4K buffer either, your call but patch is 256 bytes for the buffer.

Can you test with just one of the two changes - either force flush if len < 3, or reduce buff_size?

#17 - 07/28/2014 10:11 PM - nobu (Nobuyoshi Nakada)

Tomas Hoger wrote:

Hence the minimal reproducer should be:

```
require 'openssl'
digest = OpenSSL::Digest.new('sha1')
hmac_val = OpenSSL::HMAC.digest(digest, 'secret', 'value')
print [hmac_val].pack('m')
```

I couldn't reproduce it with that code, can you?

#18 - 07/29/2014 07:55 AM - thoger (Tomas Hoger)

Nobuyoshi Nakada wrote:

I couldn't reproduce it with that code, can you?

I can't, and I explained that the output of `OpenSSL::HMAC.digest` is way too short to fill or overflow `buff[]` in `encodes()`. It was added to make it possible for reporter to test if he can reproduce with it. No crash on that should indicate no issue in `pack/encodes`.

Will's attached patches suggest that moving `buff` from stack to heap, or significantly reducing its size solved the problem. Maybe 256 vs. 4096 is what makes a difference between exhausting and not exhausting all stack memory in his use case?

#19 - 07/30/2014 04:48 PM - wkwood (Will Wood)

Well the reproducibility issue appears to be a toolset problem. If I build with `-O2` the code works fine. I think ultimately the optimizations (O3) for gcc 4.7.2 at least with the mingw toolset are causing the issue here for windows. I've subsequently built with the mingw 4.9.1 toolset and it works fine with O3, so I guess there's a 4.7.2 gcc bug that's in the way here.

#20 - 08/01/2014 09:57 AM - pwann (Poul Wann Jensen)

This crash only triggers with `FORTIFY_SOURCE`. When calling `rb_str_buf_cat` at the end of `encodes` for the situation where the `len` variable ends up as 4. As in the example in `["a"*(3072*3-2)].pack("m3072")`. This causes 1 byte corruption of the stack, triggering `__fortify_fail` at the epilogue of `rb_str_buf_cat` and the `rb_bug` will never be executed in this case, unless it is compiled without `FORTIFY_SOURCE`.

Stack canary protection on Windows should produce the same crash I suspect, but this was tested on GCC 4.8.2.

#21 - 08/04/2014 09:15 AM - thoger (Tomas Hoger)

This seems to be getting off-topic, so just few quick notes:

- It seems `-fstack-protector*` (SSP) is what is referred to in the previous comment, not `FORTIFY_SOURCE`.
- If there is `encodes()`'s `buff[]` overflow, it corrupts `encodes()`'s SSP cookie, that is only checked on exit from `encodes()`. `rb_str_buf_cat()` called from `encodes()` after overflow does not matter, as it may or may not have its own SSP cookie, that is checked at its exit, and that's not corrupted by `buff[]` overflow. So the check leading to `rb_bug()` is still expected to happen, as the corrupted SSP cookie is only checked later.
- The first byte of the SSP cookie is expected to be `\0` on e.g. recent Linux systems (https://sourceware.org/bugzilla/show_bug.cgi?id=10149). Hence off-by-one overflow with `\0` would not be detected.

#22 - 08/04/2014 11:46 AM - nobu (Nobuyoshi Nakada)

Tomas Hoger wrote:

- The first byte of the SSP cookie is expected to be `\0` on e.g. recent Linux systems (https://sourceware.org/bugzilla/show_bug.cgi?id=10149). Hence off-by-one overflow with `\0` would not be detected.

`encodes()` does `uuencode` and `mime-encode`, so never writes `\0`.

#23 - 08/04/2014 11:55 AM - thoger (Tomas Hoger)

Nobuyoshi Nakada wrote:

`encodes()` does `uuencode` and `mime-encode`, so never writes `\0`.

Sorry, my bad - I already forgot it was `\n` that was written out of bounds, not `\0`.

#24 - 08/04/2014 12:38 PM - nobu (Nobuyoshi Nakada)

(2014/07/31 1:48), wkwood@gmail.com wrote:

Well the reproducibility issue appears to be a toolset problem. If I build with `-O2` the code works fine. I think ultimately the optimizations (O3) for gcc 4.7.2 at least with the mingw toolset are causing the issue here for windows. I've subsequently built with the mingw 4.9.1 toolset and it works fine with O3, so I guess there's a 4.7.2 gcc bug that's in the way here.

Couldn't you try the trunk?

Files

pack.patch	2.74 KB	07/09/2014	wkwood (Will Wood)
BucketTest.rb	326 Bytes	07/09/2014	wkwood (Will Wood)
pack.c.patch	769 Bytes	07/28/2014	wkwood (Will Wood)