Ruby master - Bug #17027

Connection leak possibility in Net::FTP#transfercmd

07/13/2020 10:44 AM - koshigoe (Masataka SUZUKI)

Status:	Open		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.7.1p83 (2020-03-31 revision a0c7c23c9c) [x86_64-darwin19]	**Backport:**	2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: UNKNOWN

Description

https://github.com/ruby/ruby/blob/bad7ab35d1e38f47b09f15fc5750387ac73b2286/lib/net/ftp.rb#L542-L556
https://github.com/ruby/net-ftp/blob/14d2544190f7e4b77b41a3fd0c676f5b8ebd238c/lib/net/ftp.rb#L542-L556

The connection conn may not release if exception occurred.

Reproduce

```
$ docker run --rm \
  --name vsftpd \
  -p 20-21:20-21 \
  -p 21100-21110:21100-21110 \
  -e FTP_USER=user \
  -e FTP_PASS=pass \
  -e PASV_ADDRESS=localhost \
  -e PASV_MIN_PORT=21100 \
  -e PASV_MAX_PORT=21110 \
  fauria/vsftpd

$ docker exec vsftpd ps aux | grep vsftp
root         1  0.0  0.0  11704  2580 ?        Ss   09:44   0:00 /bin/bash /usr/sbin/run-vsftpd.sh
root        13  0.0  0.1  53296  3884 ?        S    09:44   0:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

$ diff -u ~/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb.orig ~/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb.orig
--- /Users/koshigoe/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb.orig    2020-07-13 19:41:53.000000000 +0900
+++ /Users/koshigoe/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb 2020-07-13 19:42:46.000000000 +0900
@@ -549,6 +549,7 @@
           end
         end
         resp = sendcmd(cmd)
+        raise
         # skip 2XX for some ftp servers
         resp = getresp if resp.start_with?("2")
         if !resp.start_with?("1")

require 'net/ftp'

ftp = Net::FTP.new
ftp.passive = true
ftp.binary = true
ftp.connect('localhost')
ftp.login('user', 'pass')

begin
  ftp.put(__FILE__, '/uploaded-bin')
rescue
  ftp.close
  sleep 300
```

```
end

$ docker exec vsftpd ps aux | grep vsftp
root          1  0.0  0.0  11704  2580 ?        Ss   09:44   0:00 /bin/bash /usr/sbin/run-vsftpd.sh
root         13  0.0  0.1  53296  3884 ?        S    09:44   0:00 /usr/sbin/vsftpd /etc/vsftpd/vsft
pd.conf
nobody      191  0.0  0.1  75752  4420 ?        Ss   10:43   0:00 /usr/sbin/vsftpd /etc/vsftpd/vsft
pd.conf
ftp         193  0.0  0.1  75852  3768 ?        S    10:43   0:00 /usr/sbin/vsftpd /etc/vsftpd/vsft
pd.conf
```

History

#1 - 07/13/2020 10:46 AM - koshigoe (Masataka SUZUKI)

Oops
https://bugs.ruby-lang.org/issues/9872

#2 - 07/13/2020 10:51 AM - koshigoe (Masataka SUZUKI)

Fixed only about ACTIVE mode?

#3 - 07/13/2020 11:00 AM - koshigoe (Masataka SUZUKI)

Is this patch correct?
Should I close connection use shutdown and read?

```
--- /Users/koshigoe/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb.orig    2020-07-13 19:41:53.000000000 +090
0
+++ /Users/koshigoe/.rbenv/versions/2.7.1/lib/ruby/2.7.0/net/ftp.rb 2020-07-13 19:50:40.000000000 +0900
@@ -541,18 +541,23 @@
     def transfercmd(cmd, rest_offset = nil) # :nodoc:
       if @passive
         host, port = makepasv
-        conn = open_socket(host, port)
-        if @resume and rest_offset
-          resp = sendcmd("REST " + rest_offset.to_s)
-          if !resp.start_with?("3")
+        begin
+          conn = open_socket(host, port)
+          if @resume and rest_offset
+            resp = sendcmd("REST " + rest_offset.to_s)
+            if !resp.start_with?("3")
+              raise FTPReplyError, resp
+            end
+          end
+          resp = sendcmd(cmd)
+          # skip 2XX for some ftp servers
+          resp = getresp if resp.start_with?("2")
+          if !resp.start_with?("1")
             raise FTPReplyError, resp
           end
-        end
-        resp = sendcmd(cmd)
-        # skip 2XX for some ftp servers
-        resp = getresp if resp.start_with?("2")
-        if !resp.start_with?("1")
-          raise FTPReplyError, resp
+        rescue
+          conn.close if conn
+          raise
         end
       else
         sock = makeport
```

#4 - 07/13/2020 04:57 PM - jeremyevans0 (Jeremy Evans)

Your patch looks good to me. However, the net/ftp library is maintained in a separate repository. Please submit your patch as a pull request to https://github.com/ruby/net-ftp/pulls.

#5 - 07/13/2020 10:06 PM - koshigoe (Masataka SUZUKI)

https://github.com/ruby/net-ftp/pull/2