Ruby master - Bug #3337

MS-DOS device names are identified as readable_real

05/25/2010 10:49 AM - hdm (HD Moore)

Status:	Closed		
Priority:	Normal		
Assignee:	cruby-windows		
Target version:	2.6		
ruby -v:	ruby 1.9.3dev (2010-05-21 trunk 27931) [i386-mingw32]	**Backport:**	2.3: UNKNOWN, 2.4: UNKNOWN

Description

Special MS-DOS filenames return true from a call to File.readable_real? and File.file?. This exposes certain popular projects to a denial of service on the Windows platform.

```
irb(main):007:0> File.readable_real?("AUX")
=> true
```

Modifying File.file? and File.readable_real? to return false for MS-DOS device names will allow standard tests for static files to avoid MS-DOS names. The regular express below can be used to match against known MS-DOS names and should be inclusive, however a second set of eyes would be great.

```
/\/(CON|PRN|AUX|NUL|COM1|COM2|COM3|COM4|COM5|COM6|COM7|COM8|COM9|LPT1|LPT2|LPT3|LPT4|LPT5|LPT6|LPT7|LPT8|LPT9)([\.\/]|$)/i
```

If you need information on the specific projects affected by this bug, please contact me via email

History

#1 - 05/26/2010 09:55 AM - coatl (caleb clausen)

I'm not certain that the above list is complete. Among other things, windows allows programs to define their own ms-dos device names using DefineDosDevice. It might be better (at least on windows) to query the system for the list of currently defined device names.

It appears that windows ce allows device names which begin with $device or $bus.

Also, I'm puzzled by the fact that you require a / at the beginning of the device name, and allow . or / at the end. Microsoft's documentation only mentions allowing a : at the end.

I think this might be a better regexp to use (wince devices still not checked here, tho):

```
%r{\A(CON|PRN|AUX|NUL|COM[1-9]|LPT[1-9])([./:]?\z)}i
```

relevant pages on MSDN:

INFO: Understanding Device Names and Symbolic Links
http://support.microsoft.com/kb/235128

Defining an MS-DOS Device Name
http://msdn.microsoft.com/en-us/library/aa363908(VS.85).aspx

DefineDosDevice Function
http://msdn.microsoft.com/en-us/library/aa363904(VS.85).aspx

Device File Names (for windows ce)
http://msdn.microsoft.com/en-us/library/aa447463.aspx

QueryDosDevice Function (can return a list of known devices???)
http://msdn.microsoft.com/en-us/library/aa365461(v=VS.85).aspx

#2 - 05/27/2010 11:07 PM - mame (Yusuke Endoh)

- Assignee set to usa (Usaku NAKAMURA)

- Priority changed from Normal to 3

- Target version set to 2.0.0

Hi,

According to Usaku, it is difficult to fix this issue.
According to Usaku, QueryDosDevice cannot be used. It determines
some device files (such as CON) as normal file.

At least, we won't fix this issue in 1.9.2 release.
I change the target to 1.9.x and priority to Low.

Blame windows!

--
Yusuke Endoh mame@tsg.ne.jp

#3 - 05/28/2010 03:34 AM - hdm (HD Moore)

Responding to Caleb: the regex is being used to monkeypatch an application server, the leading / is because the regex is matching an incoming request, not the raw filename, and I should have clarified in the initial report.

It does seem a sticky problem to solve, but it may be possible to combine the known-bad blacklist with QueryDosDevice (.ex: CON will always be a console). I am not sure how frequently DefineDosDevice is actually used, so just filtering a known blacklist may go a long way in the short term.

#4 - 06/03/2010 10:32 AM - usa (Usaku NAKAMURA)

- Status changed from Open to Assigned

#5 - 10/31/2012 04:28 PM - usa (Usaku NAKAMURA)

- Description updated

- Target version changed from 2.0.0 to 2.6

#6 - 10/21/2017 04:18 PM - usa (Usaku NAKAMURA)

- Assignee changed from usa (Usaku NAKAMURA) to cruby-windows

#7 - 10/22/2017 02:15 AM - nobu (Nobuyoshi Nakada)

- Status changed from Assigned to Closed

- Description updated

Seems already fixed in 2.0.0.