NTFS curiosities (Part I): Short file names

Adi Oltean 27 Jan 2005 11:42 PM | 7

Aaron Stebner noted that it is possible to configure Windows to always use short file names. This is a legacy feature left over from the Windows 95 land. Sometimes, you just have to run some old MS-DOS applications. These apps will get confused about the new Windows long file names (for example, old installers). In those few cases, you don't have other choice but to really enforce short names.

But in the real world, short names can be a real pain. First of all, NTFS has to keep separate metadata information for these short names in $MFT. And sometimes you have a performance problem here: whenever you do a pattern-based file search, through the FindFirstFile/FindNextFile APIs, you have to look for **both** names (long and short), for every single file! And that's just the beginning...

Remember security?

There are sometimes subtle security implications here. Given that you can change the short name of a file, you can assign a name which is completely unintuitive. And you get a completely unintuitive behavior... For example, I created below a file called TEST.TXT, and set it short name to T.EXE:

```
Y:\garbage\test>echo SSS > test.txt

Y:\garbage\test>fsutil file setshortname test.txt T.EXE

Y:\garbage\test>dir
 Volume in drive Y is DISK_Y
 Volume Serial Number is B25A-37FC

 Directory of Y:\garbage\test

01/27/2005  05:48 PM    <DIR>          .
01/27/2005  05:48 PM    <DIR>          ..
01/27/2005  05:49 PM                 6 test.txt
               1 File(s)              6 bytes
               2 Dir(s)  26,645,819,392 bytes free

Y:\garbage\test>dir t.exe
 Volume in drive Y is DISK_Y
 Volume Serial Number is B25A-37FC

 Directory of Y:\garbage\test

01/27/2005  05:49 PM                 6 test.txt
               1 File(s)              6 bytes
               0 Dir(s)  26,645,819,392 bytes free

Y:\garbage\test>type t.exe
SSS
```

Wow! This looks pretty serious. It appears that an adversary can hide a real EXE in an innocent name, in an attempt to spoof an application or someone else. At least, you can see the short names through the "dir /X" command:

```
Y:\garbage\test>dir /X
 Volume in drive Y is DISK_Y
 Volume Serial Number is B25A-37FC

 Directory of Y:\garbage\test

01/27/2005  05:48 PM    <DIR>                       .
01/27/2005  05:48 PM    <DIR>                       ..
01/27/2005  05:49 PM                 6 T.EXE        test.txt
               1 File(s)              6 bytes
               2 Dir(s)  26,645,819,392 bytes free
```

Funny enough, running our new EXE starts... notepad.

```
Y:\garbage\test>tasklist |findstr /i notepad

Y:\garbage\test>t.exe

Y:\garbage\test>tasklist |findstr /i notepad
notepad.exe                 4140 Console                    0      3,144
K
```

Fortunately, the security threat is largely mitigated here by the privileges enforced by the API itself. The SetFileShortName API (used internally by the FSUTIL.EXE tool) requires the SE_RESTORE_NAME privilege, which is given only to local Administrators and Backup Operators. Thus, an unprivileged user will be unable to do such operations. Also, the short name is lost after copying the file. Finally, this API won't work over remote paths - you can set the short name only for files exposed on local volumes. Share access is safe.

Now, how do I reset the short name for a file? Apparently the FSULTIL FILE command doesn't allow us to remove the short name... the SETSHORTNAME option needs a non-empty string. As an anecdotic fact, a rename to a 8.3 formatted-name will remove the previous short name.

To conclude, the security risk is pretty low here. However, if you operate with files from an untrusted user that had logon access to your local machine, **don't** assume that there are no DLLs or EXEs out in a directory just by doing a dir. Use dir /X instead.

Tweaking the registry

You might ask yourself - how do I disable this feature? There is no way, unfortunately.

But still, even if you cannot disable short names, you can disable short name **generation**. In Windows NT, 2000, XP and Windows Server 2003, the short name is generated by default.

You can check whether the short name generation is enabled with the FSUTIL BEHAVIOR QUERY command:

```
C:\test>fsutil behavior query disable8dot3
disable8dot3 = 0
```

With a similar command, FSUTIL BEHAVIOR SET, you can disable or reenable this specific behavior. Note that this operation requires a reboot.

Finally, there is also a registry key that controls this behavior. For example, the KB 210638 gives the answer for NT/2000. A similar article describes this registry key for Windows Server 2003:

NtfsDisable8dot3NameCreation

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem

Data type	Range	Default value
REG_DWORD	0 | 1	0

Description

Specifies whether NTFS generates a short name in the 8.3 naming convention for long file names and for file names that contain characters from the extended character set. If the value of this entry is 0, then files can have two names: the name that the user specifies and the short name that NTFS generates. If the name that the user specifies conforms to the 8.3 naming convention, then NTFS does not generate a short name.

Changing this value does not change the file, but it does change the way that NTFS displays and manages the file. Also, files are named according to whatever rule is specified by this entry at the time of their creation; changing this entry does not alter the names of existing files.

Value	Meaning
0	NTFS creates short file names. This setting enables applications that cannot process long file names and computers that use differentcode pages code pages A means of providing support for character sets and keyboard layouts for different countries or regions. A code page is a table that relates the binary character codes used by a program to keys on the keyboard or to characters on the display. to find the files.
1	NTFS does not create short file names. Although this setting increases file performance, applications that cannot process long file names, and computers that use different code pages, might not be able to find the files.

Activation Method

You must restart Windows to make changes to this entry effective.

To end with an example, we can quickly test that short name creation is enabled by default in Windows Server 2003. Note that the short name is present only when the file name doesn't "fit" in 8.3 format.

```
C:\test>echo sss > c.txt

C:\test>echo sss > cxxxxxxxxxxxxxxx.txt

C:\test>dir /x
 Volume in drive C has no label.
 Volume Serial Number is 3826-D6D2

 Directory of C:\test
```

```
01/28/2005  11:14 AM    <DIR>                       .
01/28/2005  11:14 AM    <DIR>                       ..
01/28/2005  11:14 AM                 6              c.txt
01/28/2005  11:14 AM                 6 CXXXXX~1.TXT cxxxxxxxxxxxxxxx.txt
               2 File(s)             12 bytes
               2 Dir(s)   3,536,683,008 bytes free
```

In the end, I would recommend, whenever possible, to avoid using short names, and be aware of their problems.

[**update**: correcting a mistake in the original text stating that generation of short file names is disabled by default in XP and Windows Server 2003]

Comments

Malcolm 28 Jan 2005 12:32 AM #
You say that in Windows XP and Windows Server 2003 the short name is not generated by default. Yet the KB article you reference states that the default value for the NtfsDisable8dot3NameCreation key is 0, which means to create short filenames.

Ovidiu 28 Jan 2005 1:48 AM #
Even on Windows XP/2003, I always make sure I disable short fiile name generation with

fsutil behavior set disable8dot3 1

mikeb 28 Jan 2005 1:48 PM #
I get the same behavior for short filenames on Win2000 as on WinXP and Win2003.

If the file's 'long' filename is in 8.3 format, then no separate short name is displayed in "DIR /X"

If the file's 'long' filename exceeds the limits of 8.3, then a mangled short filename is displayed with "DIR /X":

I tested on Win2000 SP4 if that matters.

Adi Oltean 28 Jan 2005 2:20 PM #
You say that in Windows XP and Windows Server 2003 the short name is not generated by default. Yet the KB article you reference states that the default value for the NtfsDisable8dot3NameCreation key is 0, which means to create short filenames.

Sorry for the mistake. I updated the article...

atx 28 Jan 2005 4:13 PM #
that's really interesting. I learned many from this blog. Thanks Adi.

nimrod 15 Feb 2005 3:24 PM #
is there any application that can revert registry keys which contain 8.3 filepaths back to their long format?

余啊雷 13 Dec 2006 7:46 AM #
Over the time I have had this blog, I have often had occasion to say nice things about work that the