

Re: problems with latest smbfs changes on 2.4.34 and security backports

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2007-01/msg05413.html>

- *From:* Willy Tarreau <w@xxxxxx>
 - *Date:* Mon, 22 Jan 2007 10:18:16 +0100
-

Hi Santiago !

On Mon, Jan 22, 2007 at 09:54:00AM +0100, Santiago Garcia Mantinan wrote:

Hi again!

I tried to replicate the problem at home during the weekend with my laptop, but I couldn't get it to show links with previous kernels, so I guess I had something different on my samba server or similar, I'm at the real machines now so I have done the real tests and they look promising. I'm getting completely different results than those of Grant, which seems really weird.

I applied just this patch:

```
---
kernel-source-2.4.27.orig/fs/smbfs/proc.c
2007-01-19 17:53:57.247695476 -0700
+++ kernel-source-2.4.27/fs/smbfs/proc.c
2007-01-19 17:49:07.480161733 -0700
@@ -1997,7 +1997,7 @@
fattr->f_mode = (server->mnt->dir_mode
& (S_IRWXU | S_IRWXG | S_IRWXO)) |
S_IFDIR;
else if ( (server->mnt->flags &
SMB_MOUNT_FMODE) &&
!(S_ISDIR(fattr->f_mode)) )
- fattr->f_mode =
(server->mnt->file_mode & (S_IRWXU |
S_IRWXG | S_IRWXO)) | S_IFREG;
+ fattr->f_mode =
(server->mnt->file_mode & (S_IRWXU |
S_IRWXG | S_IRWXO)) | (fattr->f_mode
& S_IFMT);

}
```

Re: problems with latest smbfs changes on 2.4.34 and security backports

To an unpatched 2.4.34, the client is an IBM NetworkStation 1000 (a PowerPC based thin client), and the server is a normal amd64 based PC running 2.6.19.1, both running Debian, the client runs Sarge and the Server Etch. I'm describing this to see if differences on the architectures could be causing the differences on behaviour between my tests and Grant's.

```
client running 2.4.34 with above patch, server is running
2.6.19.2 to
eliminate it from the problem space (hopefully ;) :
grant@sempro:/home/other$ uname -r
2.4.34b
grant@sempro:/home/other$ ls -l
total 9
drwxr-xr-x 1 grant wheel 4096 2007-01-21 11:44 dir/
drwxr-xr-x 1 grant wheel 4096 2007-01-21 11:44 dirlink/
-rwxr-xr-x 1 grant wheel 15 2007-01-21 11:43 file*
-rwxr-xr-x 1 grant wheel 15 2007-01-21 11:43 filelink*
```

It seems to me that there is a difference, because filelink now appears the same size as file. It's just as if we had hard links instead of symlinks.

Here is what I did, I mounted the remote filesystem on /mnt on my client, the share on the server has a normal Debian Sarge PowerPC filesystem on it.

```
$ pwd
/mnt/usr
$ ls -l
total 0
drwxr-xr-x 1 root root 0 Feb 15 2005 X11R6
drwxr-xr-x 1 root root 0 Jan 16 2007 bin
drwxr-xr-x 1 root root 0 Jan 16 2007 doc
drwxr-xr-x 1 root root 0 Feb 10 2005 games
drwxr-xr-x 1 root root 0 Jan 16 2007 include
lrwxr-xr-x 1 root root 10 Jan 16 2007 info -> share/info
drwxr-xr-x 1 root root 0 Jan 16 2007 lib
drwxr-xr-x 1 root root 0 Feb 10 2005 local
drwxr-xr-x 1 root root 0 Jan 16 2007 sbin
drwxr-xr-x 1 root root 0 Jan 5 2006 share
drwxr-xr-x 1 root root 0 Dec 15 2004 src
$ ls -l info/
total 249856
-rwxr-xr-x 1 root root 150109 Jul 16 2004 coreutils.info.gz
-rwxr-xr-x 1 root root 1299 Jan 16 2007 dir
-rwxr-xr-x 1 root root 1299 Jan 16 2007 dir.old
-rwxr-xr-x 1 root root 28019 Mar 20 2005 find.info.gz
-rwxr-xr-x 1 root root 26136 Nov 22 2004 grep.info.gz
-rwxr-xr-x 1 root root 12914 Sep 16 2006 gzip.info.gz
```

Re: problems with latest smbfs changes on 2.4.34 and security backports

```
-rwxr-xr-x 1 root root 12316 Sep 18 2005 ipc.info.gz
-rwxr-xr-x 1 root root 21432 Jan 23 2005 rl5userman.info.gz
-rwxr-xr-x 1 root root 26647 Dec 1 2004 sed.info.gz
-rwxr-xr-x 1 root root 123382 Dec 1 2006 tar.info.gz
-rwxr-xr-x 1 root root 54876 May 23 2005 wget.info.gz
$ cd ../bin
$ ls -l sh
lrwxr-xr-x 1 root root 4 Jan 16 2007 sh -> bash
$ dd if=sh bs=1 count=6
  ELF +0 records in
 6+0 records out
 6 bytes transferred in 0.001432 seconds (4190 bytes/sec)
```

As you can see I now can see the symbolic links perfectly and they work as expected.

In fact, this patch is working so well that it poses a security risk, as now the devices on my /mnt/dev directory are not only seen as devices (like they were seen on 2.4.33) but they also work (which didn't happen on 2.4.33).

Why do you consider this a security problem ? Is any user able to create a device entry with enough permissions ? As a general rule of thumb, networked file systems should be mounted with the "nodev" option.

So... for me now the remote filesystem works as if it was a local filesystem, without any difference of behaviour, not even on special files like devices or whatever.

As I said before... this behaviour of having the remote device files work... seems a security problem and I don't think is desirable, other than that it seems to work well on my PowerPC, I'll try to run the tests on a normal x86 client and report back.

Thanks very much for your tests.

Grant, just to be sure, are you really certain that you tried the fixed kernel ? It is possible that you booted a wrong kernel during one of your tests. I'm intrigued by the fact that it changed nothing for you and that it fixed the problem for Santiago.

Best regards,
Willy

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@xxxxxxxxxxxxxxxxx
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>

Re: problems with latest smbfs changes on 2.4.34 and security backports