DragonFlyBSD - Bug #1839

Segfault, NULL pointer dereference in mount_mfs from LiveCD.

09/15/2010 02:04 PM - eocallaghan

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

By running the `reboot` command from the LiveCD one is able to get a seg fault
as follows:

syncing disks...
done
unmount(0xffffffffe0c385c60): Forced unmount: 2 namecache references still present
unmount(0xffffffffe0c385c60): Forced unmount: 4 process references still present
seg-fault accessing address 0 rip=0x40782c pid=85 p_comm=mount_mfs
EXDEV case 1 0xffffffffe010ab9b0
pid 85 (mount_mfs), uid 0: exited on signal 11

Rebooting..

We should clean that one up before release.. Although not a massive priority at
the moment.

Cheers,
Edward.

History

#1 - 09/15/2010 05:52 PM - alexh

I suggest we actually move away from mfs and use tmpfs instead. This would
involve (at least) the following steps:
- Change the fstab for the nrelease magic to use tmpfs, but keeping the same
options in use (i.e. size [note that mfs' size is in sectors, iirc])
- Probably expand mount_tmpfs to use FSCopy & FSPaste with an optional parameter
'-C', as with mount_mfs, as long as we don't have a working unionfs. FSCopy and
FSPaste can be found in newfs/fscopy.c. An alternative to this would be finally
fixing unionfs, but that's a more complicated issue.
- Test a few installations to see if everything still works as expected with the
new tmpfs magic. This would ideally include both x86 and x86_64.

Cheers,
Alex Hornung

#2 - 09/15/2010 09:53 PM - elekktretterr

>
> Alex Hornung <ahornung@gmail.com> added the comment:
>
> I suggest we actually move away from mfs and use tmpfs instead. This would
> involve (at least) the following steps:
> - Change the fstab for the nrelease magic to use tmpfs, but keeping the
> same
> options in use (i.e. size [note that mfs' size is in sectors, iirc])
> - Probably expand mount_tmpfs to use FSCopy & FSPaste with an optional
> parameter
> '-C', as with mount_mfs, as long as we don't have a working unionfs.
> FSCopy and
> FSPaste can be found in newfs/fscopy.c. An alternative to this would be
> finally
> fixing unionfs, but that's a more complicated issue.
> - Test a few installations to see if everything still works as expected
> with the
> new tmpfs magic. This would ideally include both x86 and x86_64.

>
> Cheers,
> Alex Hornung

This might be slightly inaccurate, but is it possible currently, when using LiveCD, to write to the memory filesystem? (either mfs or tmpfs). It would be great. I often had a need in the past to create temporary files.

Petr

#3 - 09/16/2010 12:23 AM - dillon

:This might be slightly inaccurate, but is it possible currently, when
:using LiveCD, to write to the memory filesystem? (either mfs or tmpfs). It
:would be great. I often had a need in the past to create temporary files.
:
:Petr

Several mount points such as /var, /tmp, and /etc are writable when booting from a LiveCD, precisely because they are using a memory filesystem (mfs, tmpfs, whatever).

Yes, it's convenient to be able to edit those even though they will reset on reboot.

-Matt
Matthew Dillon
<dillon@backplane.com>