
Subject: Re: [PATCH 0/25] Sysfs cleanups & tagged directory support
Posted by [ebiederm](#) on Wed, 08 Aug 2007 15:53:38 GMT
[View Forum Message](#) <> [Reply to Message](#)

Tejun Heo <teheo@suse.de> writes:

> Tejun Heo wrote:
>> Eric W. Biederman wrote:
>>> Tejun Heo <htejun@gmail.com> writes:
>>>
>>>> Cornelia Huck wrote:
>>>>> On Wed, 08 Aug 2007 23:35:36 +0900,
>>>>> Tejun Heo <htejun@gmail.com> wrote:
>>>>>
>>>>>> Does the attached patch happen to fix the problem?
>>>>>> Indeed it does; thanks!
>>>> Yeah, you seem to have 32bit off_t. UINT_MAX overflows, so...
>>> Weird. And we have it opening the directory O_LARGEFILE.
>>>
>>> I have no problems with the fix though.
>>
>> It's probably because of struct dirent definition used by readdir().
>
> More specifically, d_off field. It's a bit twisted. For the last
> entry, filp->f_pos gets written into the field and gets wrapped while
> being copied out to userland or in glibc.

That could do it, and glibc is crunching it. Oh well, it is
easy enough to avoid as long as our inode numbers are small which
the idr allocator seems to ensure.

Eric

Containers mailing list
Containers@lists.linux-foundation.org
<https://lists.linux-foundation.org/mailman/listinfo/containers>
