
Subject: Re: [PATCH 00/10] Containers(V10): Generic Process Containers
Posted by [Pavel Emelianov](#) on Wed, 30 May 2007 10:44:24 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi Paul.

I have faced a warning during testing your patches.
The testcase is simple:

```
# ssh to the node
mount -t container none /cnt/rss/ -o rss
mkdir /cnt/rss/0
/bin/echo $$ > /cnt/rss/0/tasks
# exit with ^d and ssh again
rmdir /cnt/rss/0
dmesg
```

BUG: at mm/slab.c:777 __find_general_cachep()
[<c04656c8>] __kmalloc+0x3f/0xa5
[<c0440e3a>] container_tasks_open+0x56/0x11f
[<c0440bcc>] container_file_open+0x0/0x36
[<c0440bfb>] container_file_open+0x2f/0x36
[<c0467a12>] __dentry_open+0xc1/0x178
[<c0467b43>] nameidata_to_filp+0x24/0x33
[<c0467b84>] do_filp_open+0x32/0x39
[<c04678eb>] get_unused_fd+0x50/0xb6
[<c0467bcd>] do_sys_open+0x42/0xbe
[<c0467c82>] sys_open+0x1c/0x1e
[<c0404c12>] sysenter_past_esp+0x5f/0x85
[<c05b0000>] __xfrm_policy_check+0x11a/0x4f6

The bug seems to be here:

```
static int container_tasks_open(struct inode *unused, struct file *file)
{
    ...
    npids = container_task_count(cont);
    pidarray = kmalloc(npids * sizeof(pid_t), GFP_KERNEL);
    if (!pidarray)
        goto err1;
    ...
}
```

The npids happened to be 0 and kmalloc warns that size is zero.

Thanks,
Pavel.
