Subject: vzctl: race condition at open("/sbin/init")
Posted by Vasily Kulikov on Wed, 25 Jul 2012 19:07:50 GMT
View Forum Message <> Reply to Message

Hi,

stat()+open() is not atomic in the code below, so there is a race condition. A container root may change /sbin/init between these calls to e.g. FIFO and then make the vzctl's process hang up on read().

I'd add O_NOCTTY to open's flags and change stat() before open() to fstat() just after open().

vzctl-3.3/src/lib/readelf.c:

```
int get_arch_from_elf(const char *file)
{
...
 if (stat(file, &st)) <<<<<
  return -1;
 if (!S_ISREG(st.st_mode))
  return -1;
 fd = open(file, O_RDONLY); <<<<<
 if (fd < 0)
  return -1;
 nbytes = read(fd, (void *) &elf_hdr, sizeof(elf_hdr));
...
}
```

Thanks,

--
Vasily