Subject: Re: [PATCH 3/3][UNIX] The unix_nr_socks limit can be exceeded
Posted by davem on Sun, 11 Nov 2007 06:08:43 GMT

View Forum Message <> Reply to Message

From: Pavel Emelyanov <xemul@openvz.org>
Date: Wed, 07 Nov 2007 17:01:17 +0300

> The unix_nr_socks value is limited with the 2 * get_max_files() value,
> as seen from the unix_create1(). However, the check and the actual
> increment are separated with the GFP_KERNEL allocation, so this limit
> can be exceeded under a memory pressure - task may go to sleep freeing
> the pages and some other task will be allowed to allocate a new sock
> and so on and so forth.
>
> So make the increment before the check (similar thing is done in the
> sock_kmalloc) and go to kmalloc after this.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

Applied, good catch Pavel.