
Subject: [PATCH] [openvz] printk: Handle global log buffer reallocation

Posted by [maximilian attems](#) on Tue, 19 Oct 2010 08:11:11 GMT

[View Forum Message](#) <> [Reply to Message](#)

From: Ben Hutchings <ben@decadent.org.uk>

Subject: [PATCH] [openvz] printk: Handle global log buffer reallocation

Date: Sun, 17 Oct 2010 02:24:28 +0100

Currently an increase in log_buf_len results in disaster, as ve0.log_buf is left pointing to the old log buffer.

Update ve0.log_buf when the global log buffer is reallocated. Also acquire logbuf_lock before reading ve_log_buf_len, to avoid a race with reallocation.

Reported-and-tested-by: Tim Small <tim@seoss.co.uk>

Signed-off-by: Ben Hutchings <ben@decadent.org.uk>

Signed-off-by: maximilian attems <max@stro.at>

belows patch fixes <http://bugs.debian.org/600299>

--- a/kernel/printk.c

+++ b/kernel/printk.c

@@ -198,6 +198,9 @@

spin_lock_irqsave(&logbuf_lock, flags);

log_buf_len = size;

log_buf = new_log_buf;

+#ifdef CONFIG_VE

+ ve0.log_buf = log_buf;

+#endif

offset = start = min(con_start, log_start);

dest_idx = 0;

@@ -354,9 +357,9 @@

if (ve_log_buf == NULL)

goto out;

count = len;

+ spin_lock_irq(&logbuf_lock);

if (count > ve_log_buf_len)

count = ve_log_buf_len;

- spin_lock_irq(&logbuf_lock);

if (count > ve_logged_chars)

count = ve_logged_chars;

if (do_clear)