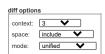
switch Linus Torvalds

log msg 💙 about summary refs log tree commit diff stats search

 author committer
 Eric Dumazet <edumazet@google.com>
 2020-02-10 11:07:21-0800

 committer
 Greg Kroah-Hartman <gregkh@linuxfoundation.org>
 2020-02-12 11:53:23-0800

 commit
 6cdled50efd88261298577cd92a14f2768eddeeb (patch)
 6cd1ed30e1d802.6129637/cd92a1412/80edddeeB (patch e5b05f21f64000849c3559cb4972d993c818fc89 3f4ef485be9d54040b695f32ec76d0flea50bbf3 (diff) linux-6cdled50efd88261298577cd92a14f2768eddeeb.



vt: vt_ioctl: fix race in VT_RESIZEX

```
We need to make sure vc_cons[i].d is not NULL after grabbing console lock(), or risk a crash.
Fixes: ldal77e4c3f4 ("Linux-2.6.12-rc2")
Signed-off-by: Eric Dumazet cedumazet@google.com>
Cc: stable cetable@yeer.kernel.org>
Reported-by: syzbot syzkaller@googlegroups.com>
Reported-by: syzbot syzkaller@googlegroups.com>
Signed-off-by: Greg Kroah-Hartman Gregkh@linuxfoundation.org>
```

Diffstat |-rw-r--r-- drivers/tty/vt/vt_ioctl.c 17 1 files changed, 11 insertions, 6 deletions

```
for (i = 0; i < MAX_NR_CONSOLES; i++) {
    struct vc_data *vcp;</pre>
                                             if (!vc_cons[i].d)
continue;
                                            continue;
console_lock();
if (v.v_vlin)
    vc_cons[i].d->vc_scan_lines = v.v_vlin;
if (v.v_clin)
    vc_cons[i].d->vc_font.height = v.v_clin;
vc_cons[i].d->vc_resize_user = 1;
vc_resize(vc_cons[i].d, v.v_cols, v.v_rows);
vcp = vc_cons[i].d;
if (vcp) (
                                             if (vcp)
                                                          vcp->vc_scan_lines = v.v_vlin;
if (v.v_clin)
                                                            vc_ciin;
vcp->vc_font.height = v.v_clin;
vcp->vc_resize_user = 1;
vc_resize(vcp, v.v_cols, v.v_rows);
                                             console unlock();
```