author 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 6cd1ed50efd88261298577cd92a14f2768eddeeb (patch)
tree e5b05f21f64000849c3559cb4972d993c818fc89
parent 3f4ef485be9d54040b695f32ec76d0f1ea50bbf3 (diff)
download linux-6cd1ed50efd88261298577cd92a14f2768eddeeb.tar.gz

diff options
context: 3
space: include
mode: unified

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.

general protection fault, probably for non-canonical address 0xdfffffc0000000068: 0000 [#1] PREEMPT SMP KASAN
KASAN: null-ptr-deref in range [0x0000000000000340-0x0000000000000347]
CPU: 1 PID: 19462 Comm: syz-executor.5 Not tainted 5.5.0-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
RIP: 0010:vt_ioctl+0x1f96/0x26d0 drivers/tty/vt/vt_ioctl.c:883
Code: 74 41 e8 bd a6 84 fd 48 89 d8 48 c1 e8 03 42 80 3c 28 00 0f 85 e4 04 00 00 48 8b 03 48 8d b8 40 03 00 00 48 89 fa 48 c1 ea 03 <42> 0f b6 14 2a 84 d2 74 09 80 fa 03 0f 8e b1 05 00 00 44 89 b8 40
RSP: 0018:ffffc900086d7bb0 EFLAGS: 00010202
RAX: 0000000000000000 RBX: ffffffff8c34ee88 RCX: ffffc9001415c000
RDX: 0000000000000068 RSI: ffffffff83f0e6e3 RDI: 0000000000000340
RBP: ffffc900086d7cd0 R08: ffff888054ce0100 R09: fffffbfff16a2f6d
R10: ffff888054ce0998 R11: ffff888054ce0100 R12: 000000000000001d
R13: dffffc0000000000 R14: 1ffff920010daf79 R15: 000000000000ff7f
FS:  00007f7d13c12700(0000) GS:ffff8880ae900000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 00007ffd477e3c38 CR3: 0000000095d0a000 CR4: 00000000001406e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 tty_ioctl+0xa37/0x14f0 drivers/tty/tty_io.c:2660
 vfs_ioctl fs/ioctl.c:47 [inline]
 ksys_ioctl+0x123/0x180 fs/ioctl.c:763
 __do_sys_ioctl fs/ioctl.c:772 [inline]
 __se_sys_ioctl fs/ioctl.c:770 [inline]
 __x64_sys_ioctl+0x73/0xb0 fs/ioctl.c:770
 do_syscall_64+0xfa/0x790 arch/x86/entry/common.c:294
 entry_SYSCALL_64_after_hwframe+0x49/0xbe
RIP: 0033:0x45b399
Code: ad b6 fb ff c3 66 2e 0f 1f 84 00 00 00 00 00 66 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 0f 83 7b b6 fb ff c3 66 2e 0f 1f 84 00 00 00 00
RSP: 002b:00007f7d13c11c78 EFLAGS: 00000246 ORIG_RAX: 0000000000000010
RAX: ffffffffffffffda RBX: 00007f7d13c126d4 RCX: 000000000045b399
RDX: 0000000020000080 RSI: 000000000000560a RDI: 0000000000000003
RBP: 000000000075bf20 R08: 0000000000000000 R09: 0000000000000000
R10: 0000000000000000 R11: 0000000000000246 R12: 00000000ffffffff
R13: 0000000000000666 R14: 00000000004c7f04 R15: 000000000075bf2c
Modules linked in:
---[ end trace 80970faf7a67eb77 ]---
RIP: 0010:vt_ioctl+0x1f96/0x26d0 drivers/tty/vt/vt_ioctl.c:883
Code: 74 41 e8 bd a6 84 fd 48 89 d8 48 c1 e8 03 42 80 3c 28 00 0f 85 e4 04 00 00 48 8b 03 48 8d b8 40 03 00 00 48 89 fa 48 c1 ea 03 <42> 0f b6 14 2a 84 d2 74 09 80 fa 03 0f 8e b1 05 00 00 44 89 b8 40
RSP: 0018:ffffc900086d7bb0 EFLAGS: 00010202
RAX: 0000000000000000 RBX: ffffffff8c34ee88 RCX: ffffc9001415c000
RDX: 0000000000000068 RSI: ffffffff83f0e6e3 RDI: 0000000000000340
RBP: ffffc900086d7cd0 R08: ffff888054ce0100 R09: fffffbfff16a2f6d
R10: ffff888054ce0998 R11: ffff888054ce0100 R12: 000000000000001d
R13: dffffc0000000000 R14: 1ffff920010daf79 R15: 000000000000ff7f
FS:  00007f7d13c12700(0000) GS:ffff8880ae900000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 00007ffd477e3c38 CR3: 0000000095d0a000 CR4: 00000000001406e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400

Fixes: 1da177e4c3f4 ("Linux-2.6.12-rc2")
Signed-off-by: Eric Dumazet <edumazet@google.com>
Cc: stable <stable@vger.kernel.org>
Reported-by: syzbot <syzkaller@googlegroups.com>
Link: https://lore.kernel.org/r/20200210190721.200418-1-edumazet@google.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

```
diff --git a/drivers/tty/vt/vt_ioctl.c b/drivers/tty/vt/vt_ioctl.c
index 8b0ed139592f9..ee6c91ef1f6cf 100644
--- a/drivers/tty/vt/vt_ioctl.c
+++ b/drivers/tty/vt/vt_ioctl.c
@@ -876,15 +876,20 @@ int vt_ioctl(struct tty_struct *tty,
                        return -EINVAL;

                for (i = 0; i < MAX_NR_CONSOLES; i++) {
+                       struct vc_data *vcp;
+
                        if (!vc_cons[i].d)
                                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 (v.v_vlin)
+                                       vcp->vc_scan_lines = v.v_vlin;
+                               if (v.v_clin)
+                                       vcp->vc_font.height = v.v_clin;
+                               vcp->vc_resize_user = 1;
+                               vc_resize(vcp, v.v_cols, v.v_rows);
+                       }
                        console_unlock();
                }
                break;
```