Date: Wed, 1 Sep 2021 17:15:57 +0800
From: Minh Yuan <yuanmingbuaa@...il.com>
To: oss-security@...ts.openwall.com
Subject: CVE-2021-3753: A out-of-bounds caused by the race of KDSETMODE in vt
 for latest Linux

Hi,

We recently discovered a race oob read in vt in the latest kernel (
v4.19.205 for now), and the patch
<https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=ffb324e6f874121f7dce5bdae5e05d02baae7269>
can't
handle this bug.

The root cause of this vulnerability is that the write access to vc_mode is
not protected by lock in vt_ioctl (KDSETMDE).
To trigger the oob, we set the crafted vc_visible_origin by using the
following steps:

```
  Thread 1                                        Thread 2
                                                                Thread
3
vt_ioctl()
    case KDSETMODE:
        vc->vc_mode = KD_GRAPHICS

                                            vt_ioctl()
                                                case TIOCL_BLANKSCREEN:
                                                    if (
vc->vc_mode != KD_TEXT)

console_blanked = fg_console + 1;
                                                ... ...
                                                case VT_RESIZE
                                                    set_origin()
                                                        vgacon_set_origin()

// make vc_visible_origin not equal to vga_vram_base
                                                            if (
console_blanked && !vga_palette_blanked)
                                                                return 0;



                                                 vt_ioctl()

                                                     case
KDSETMODE:


vc->vc_mode = KD_TEXT

                                            write()
                                                do_con_write()
                                                    do_con_troll()
                                                        lf()
                                                            con_scroll()

// set vga_rolled_over
                                                                vgacon_scroll()
                                                                    if (
c->vc_mode != KD_TEXT)

return false;

oldo = c->vc_origin;

vga_rolled_over = oldo - vga_vram_base;

                                            vt_ioctl()
                                                case TIOCL_SCROLLCONSOLE:
wrap = rolled_over + c->vc_size_row

// set vc_visible_origin to oob
                                                        c->vc_
visible_origin = vga_vram_base + (from + from_off) % wrap

                                                case TIOCL_SETSEL:
                                                    // trigger oob
                                                    sel_pos(ps)









console_lock();

                                                            ...

console_unlock();


        console_lock();
        ...
        console_unlock();
```

And the patch for this issue is available now. (
https://github.com/torvalds/linux/commit/2287a51ba822384834dafc1c798453375d1107c7
)

Timeline:
* 08.30.21 - Vulnerability reported to security@...nel.org.
* 08.31.21 - CVE-2021-3753 assigned.
* 09.01.21 - Vulnerability opened.

Regards,

Yuan Ming, Tsinghua University