Bug 206357 - Linux Kernel 5.4.7 - vgacon_invert_region use-after-free

Status: NEW
Alias: None
Product: Drivers
Component: Console/Framebuffers (show other bugs)
Hardware: All Linux
Importance: P1 normal
Assignee: James Simmons
URL:
Keywords:
Depends on:
Blocks:

Reported: 2020-01-30 16:39 UTC by Tristan Madani
Modified: 2020-03-30 04:13 UTC (History)
CC List: 1 user (show)
See Also:
Kernel Version: 5.4.7
Tree: Mainline
Regression: No

Attachments

Add an attachment (proposed patch, testcase, etc.)

Tristan Madani 2020-01-30 16:39:00 UTC Description

```
Linux Kernel 5.4.7 - vgacon_invert_region use-after-free

0x01 - Introduction
===

# Product: Linux Kernel
# Version: 5.4.7 and probably other versions
# Bug: UAF (Read)
# Tested on: GNU/Linux Debian 9 x86_64


0x02 - Details
===

There is a UAF read in the vgacon_invert_region function from the low level VGA
based console driver.

Code analysis (drivers/video/console/vgacon.c):

static void vgacon_invert_region(struct vc_data *c, u16 * p, int count)
{
        const bool col = vga_can_do_color;

        while (count--) {
                u16 a = scr_readw(p);           // <-- UAF occurs here
                if (col)
                        a = ((a) & 0x88ff) | (((a) & 0x7000) >> 4) |
                            (((a) & 0x0700) << 4);
                else
                        a ^= ((a & 0x0700) == 0x0100) ? 0x7000 : 0x7700;
                scr_writew(a, p++);
        }
}


0x03 - Crash report
===


BUG: KASAN: use-after-free in vgacon_invert_region+0x106/0x110
drivers/video/console/vgacon.c:669
Read of size 2 at addr ffff88800027917e by task syz-executor.6/22260

CPU: 3 PID: 22260 Comm: syz-executor.6 Not tainted 5.4.7 #1
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.12.0-1 04/01/2014
Call Trace:
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0xee/0x16e lib/dump_stack.c:118
 print_address_description.constprop.8+0x36/0x50 mm/kasan/report.c:374
 __kasan_report.cold.11+0x1a/0x3a mm/kasan/report.c:506
 kasan_report+0xe/0x20 mm/kasan/common.c:634
 vgacon_invert_region+0x106/0x110 drivers/video/console/vgacon.c:669
 invert_screen+0x184/0x5f0 drivers/tty/vt/vt.c:763
 highlight drivers/tty/vt/selection.c:53 [inline]
 set_selection_kernel+0xa0d/0x13b0 drivers/tty/vt/selection.c:298
 set_selection_user+0x94/0xe0 drivers/tty/vt/selection.c:177
 tioclinux+0x331/0x4e0 drivers/tty/vt/vt.c:3039
 vt_ioctl+0x1bcf/0x28d0 drivers/tty/vt/vt_ioctl.c:364
 tty_ioctl+0x525/0x15a0 drivers/tty/tty_io.c:2657
 vfs_ioctl fs/ioctl.c:47 [inline]
 file_ioctl fs/ioctl.c:510 [inline]
 do_vfs_ioctl+0x1c5/0x1310 fs/ioctl.c:697
 ksys_ioctl+0x9b/0xc0 fs/ioctl.c:714
 __do_sys_ioctl fs/ioctl.c:721 [inline]
 __se_sys_ioctl fs/ioctl.c:719 [inline]
 __x64_sys_ioctl+0x6f/0xb0 fs/ioctl.c:719
 do_syscall_64+0xbc/0x560 arch/x86/entry/common.c:290
 entry_SYSCALL_64_after_hwframe+0x49/0xbe
RIP: 0033:0x4662e9
Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 73 01 c3 48 c7
c1 bc ff ff ff f7 d8 64 89 01 48
RSP: 002b:00007ff667844c68 EFLAGS: 00000246 ORIG_RAX: 0000000000000010
RAX: ffffffffffffffda RBX: 0000000000052bf00 RCX: 00000000004662e9
RDX: 0000000020000200 RSI: 000000000000541c RDI: 0000000000000003
RBP: 00000000ffffffff R08: 0000000000000000 R09: 0000000000000000
R10: 0000000000000000 R11: 0000000000000246 R12: 00000000004a744b
R13: 00000000004edd18 R14: 00000000004ac84e R15: 00007ff6678456bc

The buggy address belongs to the page:
page:ffffea0000009e40 refcount:0 mapcount:0 mapping:0000000000000000 index:0x1
raw: 0000000000000000 dead000000000100 dead000000000122 0000000000000000
raw: 0000000000000001 0000000000000000 00000000ffffffff 0000000000000000
page dumped because: kasan: bad access detected

Memory state around the buggy address:
 ffff888000279000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 ffff888000279080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
>ffff888000279100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
                                                 ^
 ffff888000279180: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
 ffff888000279200: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
==================================================================
```

wmealing 2020-03-30 04:13:59 UTC Comment 1

```
In case anyone was following along, this was assigned CVE-2020-8649

I think that this was fixed here:
```

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=513dc792d6060d5ef572e43852683097a8420f56

Note

You need to log in before you can comment on or make changes to this bug.