CVE-2020-20250

Description

The `lcdstat` process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the `lcdstat` process due to NULL pointer dereference.

Against stable `6.46.5`, the poc resulted in the following crash captured by `gdb`.

```
Thread 2.1 "lcdstat" received signal SIGSEGV, Segmentation fault.
=> 0x80562c6:   mov    BYTE PTR [edx+eax*1],bl
   0x80562c9:   mov    ebx,esi
   0x80562cb:   mov    BYTE PTR [edx+eax*1+0x1],bl
   0x80562cf:   mov    ebx,edi
0x080562c6 in ?? ()
(gdb) i r
eax            0x0      0
ecx            0x0      0
edx            0x0      0
ebx            0x0      0
esp            0x7fd8cb2c       0x7fd8cb2c
ebp            0x7fd8cb48       0x7fd8cb48
esi            0xff0000 16711680
edi            0xff000000       -16777216
eip            0x80562c6        0x80562c6
eflags         0x10246  [ PF ZF IF RF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
(gdb) info inferiors
  Num  Description       Executable
  1    <null>            target:/nova/bin/lcdstat
* 2    process 635       target:/nova/bin/lcdstat
```

And the crash dump in `/rw/logs/backtrace.log` was:

```
# cat /rw/logs/backtrace.log
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0: /nova/bin/lcdstat
2020.06.04-15:48:13.77@0: --- signal=11 --------------------------------------------
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0: eip=0x080562c6 eflags=0x00010246
2020.06.04-15:48:13.77@0: edi=0xff000000 esi=0x00ff0000 ebp=0x7fd8cb48 esp=0x7fd8cb2c
2020.06.04-15:48:13.77@0: eax=0x00000000 ebx=0x00000000 ecx=0x00000000 edx=0x00000000
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0: maps:
2020.06.04-15:48:13.77@0: 08048000-0807e000 r-xp 00000000 00:0c 1054       /nova/bin/lcdstat
2020.06.04-15:48:13.77@0: 776be000-776f3000 r-xp 00000000 00:0c 964        /lib/libuClibc-0.9.33.2.so
2020.06.04-15:48:13.77@0: 776f7000-77711000 r-xp 00000000 00:0c 960        /lib/libgcc_s.so.1
2020.06.04-15:48:13.77@0: 77712000-77721000 r-xp 00000000 00:0c 944        /lib/libuc++.so
2020.06.04-15:48:13.77@0: 77722000-7772a000 r-xp 00000000 00:0c 950        /lib/libubox.so
2020.06.04-15:48:13.77@0: 7772b000-77777000 r-xp 00000000 00:0c 946        /lib/libumsg.so
2020.06.04-15:48:13.77@0: 7777d000-77784000 r-xp 00000000 00:0c 958        /lib/ld-uClibc-0.9.33.2.so
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0: stack: 0x7fd8d000 - 0x7fd8cb2c
2020.06.04-15:48:13.77@0: 00 00 00 00 00 00 00 01 80 c1 77 77 01 00 00 00 38 d4 d8 7f 50 5f 08 08 a8 5c 08 08 78 cb d8 7f
2020.06.04-15:48:13.77@0: 79 a2 05 08 78 36 08 08 00 00 00 00 00 de 77 77 8f cf d8 7f ff ff ff ff a8 5d 08 08 00 36 08 08
2020.06.04-15:48:13.77@0:
2020.06.04-15:48:13.77@0: code: 0x80562c6
2020.06.04-15:48:13.77@0: 88 1c 02 89 f3 88 5c 02 01 89 fb 88 5c 02 02 05
```

Affected Version

This vulnerability was initially found in long-term `6.44.6`, and was fixed in stable `6.47`.

Timeline

- 2020/03/11 - reported the vulnerability to the vendor

- 2020/06/02 - the vendor fixed it in stable `6.47`
- 2021/05/04 - CVE was assigned