cq674350529 add new CVEs History

1 contributor

78 lines (67 sloc) | 3.2 KB

CVE-2020-20252

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.
=> 0x805b566:   cmp    BYTE PTR [eax+0x8],0x0
   0x805b56a:   jne    0x805b578
   0x805b56c:   push   edx
   0x805b56d:   push   edx
0x0805b566 in ?? ()
(gdb) i r
eax            0x0      0
ecx            0x807f14c        134738252
edx            0x1      1
ebx            0x7fc106c8       2143356616
esp            0x7fc0fc70       0x7fc0fc70
ebp            0x7fc0fca8       0x7fc0fca8
esi            0x8085bf8        134765560
edi            0x8085e70        134766192
eip            0x805b566        0x805b566
eflags         0x10202  [ 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 731       target:/nova/bin/lcdstat
```

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

```
# cat /rw/logs/backtrace.log
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0: /nova/bin/lcdstat
2020.06.04-15:58:23.76@0: --- signal=11 ------------------------------------------
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0: eip=0x0805b566 eflags=0x00010202
2020.06.04-15:58:23.76@0: edi=0x08085e70 esi=0x08085bf8 ebp=0x7fc0fca8 esp=0x7fc0fc70
2020.06.04-15:58:23.76@0: eax=0x00000000 ebx=0x7fc106c8 ecx=0x0807f14c edx=0x00000001
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0: maps:
2020.06.04-15:58:23.76@0: 08048000-0807e000 r-xp 00000000 00:0c 1054       /nova/bin/lcdstat
2020.06.04-15:58:23.76@0: 77680000-776b5000 r-xp 00000000 00:0c 964        /lib/libuClibc-0.9.33.2.so
2020.06.04-15:58:23.76@0: 776b9000-776d3000 r-xp 00000000 00:0c 960        /lib/libgcc_s.so.1
2020.06.04-15:58:23.76@0: 776d4000-776e3000 r-xp 00000000 00:0c 944        /lib/libuc++.so
2020.06.04-15:58:23.76@0: 776e4000-776ec000 r-xp 00000000 00:0c 950        /lib/libubox.so
2020.06.04-15:58:23.76@0: 776ed000-77739000 r-xp 00000000 00:0c 946        /lib/libumsg.so
2020.06.04-15:58:23.76@0: 7773f000-77746000 r-xp 00000000 00:0c 958        /lib/ld-uClibc-0.9.33.2.so
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0: stack: 0x7fc10000 - 0x7fc0fc70
2020.06.04-15:58:23.76@0: e4 9a 73 77 58 fe c0 7f a8 fc c0 7f 00 00 00 00 58 fe c0 7f 73 00 00 00 9c fc c0 7f 22 ac 70 77
2020.06.04-15:58:23.76@0: 58 fe c0 7f 72 00 00 08 b8 fc c0 7f 5c fd c0 7f 70 5e 08 08 c8 06 c1 7f c8 fc c0 7f ab b8 05 08
2020.06.04-15:58:23.76@0:
2020.06.04-15:58:23.76@0: code: 0x805b566
2020.06.04-15:58:23.76@0: 80 78 08 00 75 0c 52 52 50 53 e8 91 e7 ff ff 83
```

Affected Version

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

Timeline

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

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