CVE-2020-20231

Description

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

Against stable `6.46.5`, the poc resulted in the following crash dump.

```
# cat /rw/logs/backtrace.log
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0: /nova/bin/detnet
2020.06.22-16:22:09.85@0: --- signal=11 ------------------------------------------
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0: eip=0x776d86da eflags=0x00010216
2020.06.22-16:22:09.85@0: edi=0x7fe6cea4 esi=0x7fe6ce0c ebp=0x7fe6cda8 esp=0x7fe6cda0
2020.06.22-16:22:09.85@0: eax=0x00000020 ebx=0x77707ae4 ecx=0x0805d898 edx=0x7fe6cddc
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0: maps:
2020.06.22-16:22:09.85@0: 08048000-08058000 r-xp 00000000 00:0c 1062       /nova/bin/detnet
2020.06.22-16:22:09.85@0: 77630000-77665000 r-xp 00000000 00:0c 964        /lib/libuClibc-0.9.33.2.so
2020.06.22-16:22:09.85@0: 77669000-77683000 r-xp 00000000 00:0c 960        /lib/libgcc_s.so.1
2020.06.22-16:22:09.85@0: 77684000-77693000 r-xp 00000000 00:0c 944        /lib/libuc++.so
2020.06.22-16:22:09.85@0: 77694000-776b1000 r-xp 00000000 00:0c 947        /lib/libucrypto.so
2020.06.22-16:22:09.85@0: 776b2000-776ba000 r-xp 00000000 00:0c 950        /lib/libubox.so
2020.06.22-16:22:09.85@0: 776bb000-77707000 r-xp 00000000 00:0c 946        /lib/libumsg.so
2020.06.22-16:22:09.85@0: 7770d000-77714000 r-xp 00000000 00:0c 958        /lib/ld-uClibc-0.9.33.2.so
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0: stack: 0x7fe6d000 - 0x7fe6cda0
2020.06.22-16:22:09.85@0: 20 00 00 00 dc cd e6 7f f8 cd e6 7f 32 ff 04 08 dc cd e6 7f 20 00 00 00 00 00 00 00 64 a9 6d 77
2020.06.22-16:22:09.85@0: 9c d5 05 08 98 d8 05 08 e8 cd e6 7f 44 ad 6d 77 a4 ce e6 7f 02 00 00 08 f8 cd e6 7f 1c ad 6d 77
2020.06.22-16:22:09.85@0:
2020.06.22-16:22:09.85@0: code: 0x776d86da
2020.06.22-16:22:09.85@0: 8b 00 89 02 3b 83 34 ff ff ff 74 03 ff 40 24 80
```

Affected Version

This vulnerability was initially found in long-term `6.44.6`, and it seems that the latest stable version `6.48.3` still suffers from this vulnerability.

Timeline

- 2020/04/20 - reported the vulnerability to the vendor
- 2020/04/23 - the vendor confirmed the vulnerability and will work on them
- 2021/05/04 - CVE was assigned