CVE-2020-20249

Description

The `resolver` process suffers from a memory corruption vulnerability. By sending a crafted packet, an authenticated remote user can crash the `resolver` process due to invalid memory access.

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

```
# cat /rw/logs/backtrace.log
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0: /nova/bin/resolver
2020.06.19-10:32:37.42@0: --- signal=11 ------------------------------------------
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0: eip=0x7774c049 eflags=0x00010212
2020.06.19-10:32:37.42@0: edi=0x080619d0 esi=0x7f8bd684 ebp=0x7f8bd5a8 esp=0x7f8bd59c
2020.06.19-10:32:37.42@0: eax=0x00000001 ebx=0x777544ec ecx=0x08061c60 edx=0x08061c60
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0: maps:
2020.06.19-10:32:37.42@0: 08048000-0805c000 r-xp 00000000 00:0c 995        /nova/bin/resolver
2020.06.19-10:32:37.42@0: 776f1000-77726000 r-xp 00000000 00:0c 964        /lib/libuClibc-0.9.33.2.so
2020.06.19-10:32:37.42@0: 7772a000-77744000 r-xp 00000000 00:0c 960        /lib/libgcc_s.so.1
2020.06.19-10:32:37.42@0: 77745000-77754000 r-xp 00000000 00:0c 944        /lib/libuc++.so
2020.06.19-10:32:37.42@0: 77755000-7775d000 r-xp 00000000 00:0c 950        /lib/libubox.so
2020.06.19-10:32:37.42@0: 7775e000-777aa000 r-xp 00000000 00:0c 946        /lib/libumsg.so
2020.06.19-10:32:37.42@0: 777b0000-777b7000 r-xp 00000000 00:0c 958        /lib/ld-uClibc-0.9.33.2.so
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0: stack: 0x7f8be000 - 0x7f8bd59c
2020.06.19-10:32:37.42@0: 08 d6 8b 7f b4 d5 8b 7f ec d5 8b 7f c8 d5 8b 7f f1 ef 04 08 ec d5 8b 7f 60 1c 06 08 08 d6 8b 7f
2020.06.19-10:32:37.42@0: f1 16 05 08 ec d5 8b 7f 2e 00 00 00 08 d6 8b 7f 03 17 05 08 e8 71 72 77 04 d6 8b 7f 57 1b 7b 77
2020.06.19-10:32:37.42@0:
2020.06.19-10:32:37.42@0: code: 0x7774c049
2020.06.19-10:32:37.42@0: 8b 10 01 c2 83 c2 04 52 83 c0 04 50 ff 75 08 e8
```

Affected Version

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

Timeline

- 2020/01/06 - reported the vulnerability to the vendor
- 2020/01/07 - the vendor reproduced and confirmed the vulnerability
- 2021/05/04 - CVE was assigned