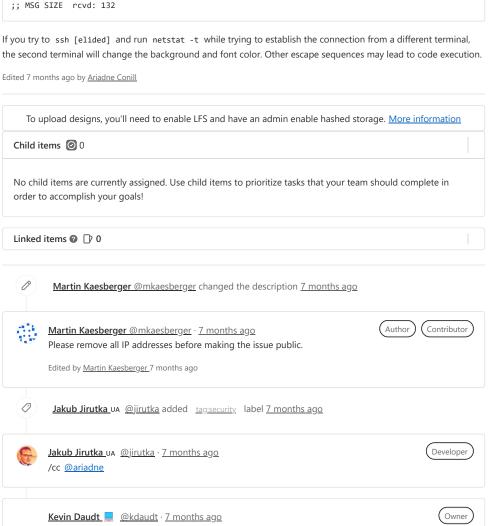
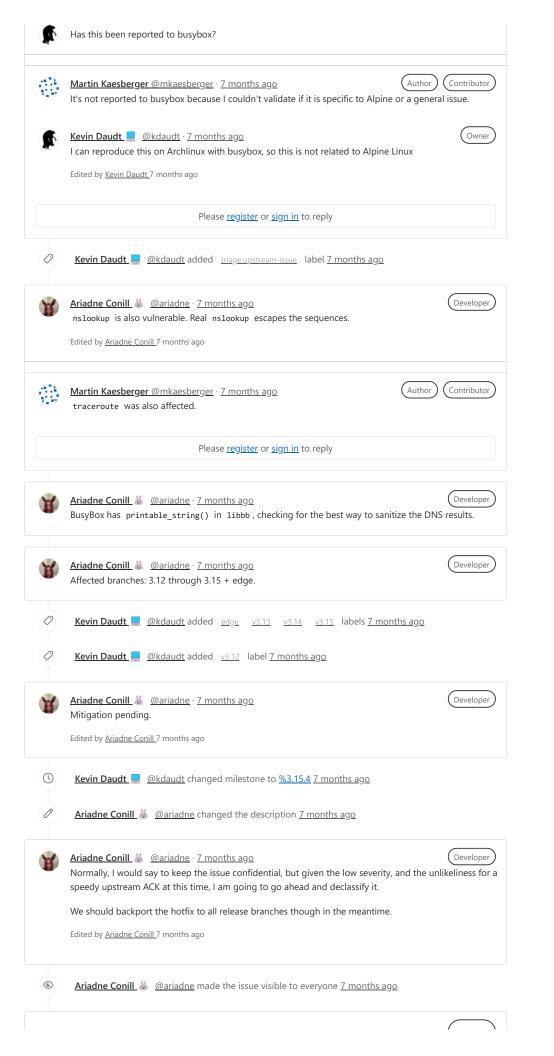
## netstat is vulnerable to escape sequence injection (busybox)

Hey there,

Alpine ships BusyBox with the netstat applet enabled. This is vulnerable to escape sequence injection when used from an VT compatible terminal. To exploit this vulnerability the PTR for a remote host must contain a escape sequence and the victim has to execute netstat. I've set up an example at [elided] with the PTR resolving to \027[33\;46mlocalhost.

```
$ dig -x [elided] @8.8.8.8
; <<>> DiG 9.16.25 <<>> -x [elided] @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59625
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;[elided]. IN PTR
;; ANSWER SECTION:
[elided]. 1 IN PTR 027[33];46mlocalhost.
;; Query time: 55 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Apr 03 00:11:16 DST 2022
;; MSG SIZE rcvd: 132
```







Please <u>register</u> or <u>sign in</u> to reply