# D-Link GO-RT-AC750 contains command injection vulnerability

## overview

- type: command injection Vulnerability
- supplier: D-Link (
- product: D-Link Go-RT-AC750
-

- affect version:  revA 1.01b03 & revB 2.00b02

The dlinkgo GO-RT-AC750 Wireless AC750 Dual-Band Easy Router is an affordable yet powerful wireless networking solution which combines the latest high-speed 802.11ac Wi-Fi specification with dual-band technology and fast Ethernet ports to deliver a seamless networking experience. The increased range and reliability of wireless AC technology reaches farther into your home, and the GO-RT-AC750's advanced security features keep your network and data safe from intruders.

## Description

### 1. Vulnerability Details

the vulnerability is in **/cgibin, hnap_main,**  the `sprintf` and `system` causes this vulnerability

```
if ( sub_41173C(v27, "/etc/templates/hnap//.shell_action") )
  sprintf(v27, "sh %s%s.sh > /dev/console &", "/var/run/", v9);
else
  sprintf(v27, "sh %s%s.sh > /dev/console", "/var/run/", v9);
system(v27);
```

we can control `v9`.

```
v5 = getenv("HTTP_SOAPACTION");
v6 = getenv("REQUEST_METHOD");
if ( v5 )
{
  if ( !strstr(v5, "http://purenetworks.com/HNAP1/GetDeviceSettings") && sub_411490(v4) < 0 )
  {
    cgibin_parse_request(0, 0, 0);
    v7 = -2;
    sub_4119C8();
    goto LABEL_36;
  }
}
else
{
  v5 = "http://purenetworks.com/HNAP1/GetDeviceSettings";
}
v8 = strrchr(v5, '/');
v9 = v8 + 1;
```