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

this vulnerability is in **cgibin, ssdpcgi_main**

```
  v11 = strncmp(v2, "urn:", 4u) != 0;
  result = 0;
  if ( v11 )
    return result;
  if ( strstr(v2, ":device:") )
  {
    lxmldbc_system("%s devices %s:%s %s %s &", "/etc/scripts/upnp/M-SEARCH.sh", v3, v12, v5, v2);
    return 0;
  }
  if ( strstr(v2, ":service:") )
  {
    lxmldbc_system("%s services %s:%s %s %s &", "/etc/scripts/upnp/M-SEARCH.sh", v3, v12, v5, v2);
    return 0;
  }
  result = 0;
}
```

`v2` is `HTTP_ST` and we can control it from http request.

```
{
  v2 = getenv("HTTP_ST");
  v3 = getenv("REMOTE_ADDR");
  v12 = getenv("REMOTE_PORT");
  v4 = getenv("SERVER_ID");
```


the `lxmldbc_system` erability