D-Link GO-RT-AC750 contains buffer overflow vulnerability

Overview

- type: buffer overflow 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**, it calls `strcpy(v27, v9)` . `v27` is on the stack and there is no size check, so there is buffer overflow vulnerability.

```
xmldoc_epnp(0, 0, v25, stdout);
sobj_del(v23);
strcpy(v27, v9);
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);
lockf(v12, 2, 0);
```

2. Recurring loopholes and POC

In order to reproduce the vulnerability, the following steps can be followed:

Start frimware through QEMU system or other methods (real device)

Run this poc