# AC系列路由器存在逻辑漏洞

在校学生，第一次挖漏洞&交cnvd，写的不到位的地方还希望审报告的师傅能够及时指正，拜谢Orz（联系邮箱：2313696342@qq.com）

检索了cve关于AC8系列的47个漏洞，确定没有重复

已通过现实场景测试确定AC8v4 V16.03.34.06以及AC21 V16.03.08.16存在该漏洞。

至少以存在该漏洞的版本：

<https://tenda.com.cn/material/show/3518> 【AC8 v4 升级软件\_V16.03.34.06】

<https://tenda.com.cn/material/show/3742> 【AC21 升级软件\_V16.03.08.16】

### 漏洞危害举例

在多用户同时登录存在该漏洞的AC系列路由器的场景下，某一恶意用户利用该漏洞，将导致需要密码连接的路由器设置为开放状态（无需密码即可连接），同时使得连接该路由器的所有设备下线。

## 漏洞分析

在/goform/WifiBasicSet下，formWifiBasicSet函数的sub\_45F3E8依次经过下面的函数，

sub\_45F3E8 -> sub\_45E1C4 -> sub\_45DC58

当我们访问/goform/WifiBasicSet，同时不设置任何参数，将导致security参数默认为none，进而程序将进入第28行的else语句，设置bss\_security的值为none，之后程序继续运行，整体表现为，路由器将无需密码即可登录，原来上线的设备下线，需要重新连接。



## 漏洞复现

连接到任意存在该漏洞的路由器，进入到tenda路由器管理界面，浏览器访问如下poc给出的链接，即可复现。

POC:[http://tendawifi.com](http://tendawifi.com" \t "_blank)/goform/WifiBasicSet