

Shenzhen Skyworth RN510 Information Disclosure

Authored by [Kaustubh G. Padwad](#)

Posted [May 4, 2021](#)

Shenzhen Skyworth RN510 suffers from an unauthenticated sensitive information disclosure vulnerability.

tags | [exploit](#), [info disclosure](#)

advisories | [CVE-2021-25326](#)

SHA-256 | [7f226e9706a9282668f82475d29e2552e812bbb3bd068893eb424f30e0d699c6d](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

Overview

Title:- Unauthenticated Sensitive information Discloser in RN510 Mesh Extender.
CVE-ID :- CVE-2021-25326
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

XSA-Dev-0012

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, RN510provides a stable & reliable high speed wired and wireless connectivity for home user and SOHO users. Utilizing state of art EasyMesh solution, two or more RN510 units could be easily teamed upwith Skyworth ONT gateway (e.g. ON543) 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, eliminate weak signal areas once and for all. RN510 work 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 2,600 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 major internet service provider (ISP) and modem. Parental Controls limits online time and block inappropriate websites according to unique profiles created for each family member. Setup is easier than ever with the Skywifi app there to walk you through every step.

Description:

An issue was discovered on Shenzhen Skyworth

Application reveals the below Sensitive information by calling http://192.168.2.1/cgi-bin/test_version.asp in without any authentication

```
2.4G SSID: SKYW_MESH_750
2.4G password: 12345678
5G SSID: SKYW_MESH_750
5G password: 12345678
username: admin
web_passwd: kaustubh
```

Additional Information

[Affected Component]

Iphddr function on page /cgi-bin/app-staticIP.asp inside the bos 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-routedad.asp and /cgi-bin/sec-urfilter.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 XSSRF.

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@se.com
* <https://s3curityb3ast.github.io/>
* <https://twitter.com/s3curityb3ast>
* <https://breakthesec.com>
* <https://www.linkedin.com/in/kaustubhpadwad>

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

[Login](#) or [Register](#) to add favorites

[Spoof](#) (2,166) [SUSE](#) (1,444)
[SQL Injection](#) (16,102) [Ubuntu](#) (8,199)
[TCP](#) (2,379) [UNIX](#) (9,159)
[Trojan](#) (686) [UnixWare](#) (185)
[UDP](#) (876) [Windows](#) (6,511)
[Virus](#) (662) [Other](#)
[Vulnerability](#) (31,136)
[Web](#) (9,365)
[Whitepaper](#) (3,729)
[x86](#) (946)
[XSS](#) (17,494)
[Other](#)



© 2022 Packet Storm. All rights reserved.

Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

About Us

[History & Purpose](#)

[Contact Information](#)


[Terms of Service](#)


[Privacy Statement](#)

[Copyright Information](#)

Hosting By

[Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)