



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



KSA-Dev-0012:CVE-2021-25326:Unauthenticated Sensitive information Discloser in Skyworth RN510 Mesh Extender

From: Kaustubh Padwad via Fulldisclosure <fulldisclosure () seclists org>
Date: Sat, 1 May 2021 20:05:15 +0000

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
=====

KSA-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, RN510 provides 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 up with Skyworth ONT gateway (e.g. GN543) 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 2,800 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 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 Skywififi 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: I2345678
5G SSID:       SKYW_MESH_750
5G password:   I2345678
username:      admin
web_passwd:    kaustubh
```

Additional Information

=====

[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 achieve XSS.

[Vulnerability Type]

=====

CSRF, XSS

How to Reproduce: (POC):

=====

One can use below exploit

Attacker needs to run above requests in order to achieve 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://s3curitvb3ast.github.io/>
* <https://twitter.com/s3curitvb3ast>
* <http://breaktheseccom>
* <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-0012:CVE-2021-25326:Unauthenticated Sensitive information Discloser 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		