

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II)

Islamabad 20 July, 2018

Subject: Advisory - Prevention Against Threats Posed by Wireless Router (Advisory No 144)

1. Introduction. Wireless Routers poses serious Security threats as it may allow anyone in close proximity to access your complete network and monitor traffic by hacking the router.
2. Technical Analysis.
 - a. Security vulnerabilities are found in open source firmware components, details are as under:-
 - (1) WPA2 (KRACK) - Key reinstallation attack.
 - (2) ffmpeg - Denial of Service.
 - (3) openssl - DoS, buffer overflow and remote code execution.
 - (4) Samba - Remote code execution.
 - b. Wireless routers are also open to direct cyber-attacks where hackers can gain illegitimate access and perform malicious activities, details are as under:-
 - (1) Man-in-the-Middle attack.
 - (2) Brute force attack.
 - (3) Rogue Access Points.
 - (4) Endpoint Attacks.
 - (5) Packet Analyzers.
 - (6) Evil Twins.
3. Affected Product Versions. All wireless routers from firms like TP Link, Linksys, Net gear etc.
4. Release of New Wi - Fi Security Feature.
 - a. Security researchers uncovered a severe flaw protocol, dubbed KRACK (Key Reinstallation Possible for attackers to intercept, decrypt and Even manipulate WiFi network traffic.
 - b. The Wi-Fi Alliance has launched WPA3 - the next-generation Wi-Fi security Standard to eliminate all the known security vulnerabilities and wireless attacks eg KRACK attacks.
 - c. WPA3 security standard will replace the existing WPA2.
 - d. Key features provided by the new protocol are as under:-
 - (1) Protection against Brute-Force Attacks.
 - (2) Protecting Public / Open Wi-Fi Networks.
 - (3) Strong Encryption for Critical Networks.

5. **Mitigation Measures.** Following best practices are suggested in this regard:-
- a. Ensure installation of **latest version** of the firmware **and strong password** access to network routers.
 - b. Disable router's remote administration feature and **hardcode "1.1.1.1."** DNS server IP address into the operating system network settings.
 - c. It is advised to make sure the sites you are visiting has **HTTPS enabled.**
 - d. Keep all the softwares, browsers and operating system **up-to-date.**
 - e. Change the name of your **default** home network (**SSID**).
 - f. Make sure you set a **strong** and unique **password** to secure your wireless network.
 - g. **Turn off** the wireless home network when not in use.
 - h. Change your **default IP** address on the Wireless router.
 - i. Always apply the latest security patches to ensure no security hole is left open to malicious actors.
 - j. **Wi - Fi** encryption should be **WPA3** with **AES** and your **Wi-Fi** password should be at last **14 characters long.**
 - k. Test your router for **open parts** using some **online testers** and block all open ports.
 - l. **Turning off** features you are not using reduces the attack surface. Turn of following features:-
 - (1) Remote Management, Remote GUI or Web Access from WAN.
 - (2) SNMP, NAT - PMP and Telnet access to the router.
 - (a) WPS.
 - (b) Ping reply
 - (c) DHCP Functionality.
6. **Recommendations.**
- a. **Install and update well reputed antiviruses** such as 'Kaspersky, Avira, Avast etc.
 - b. Always follow mitigation measures discussed at para 4
 - c. Update all softwares including Windows OS, Microsoft Office and disable macros.
 - d. Don't download attachments from untrusted sources.
7. Forwarded for perusal and dissemination of information to all concerned, please.


Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560