Pakistan Telecom Authority Headquarters, Islamabad

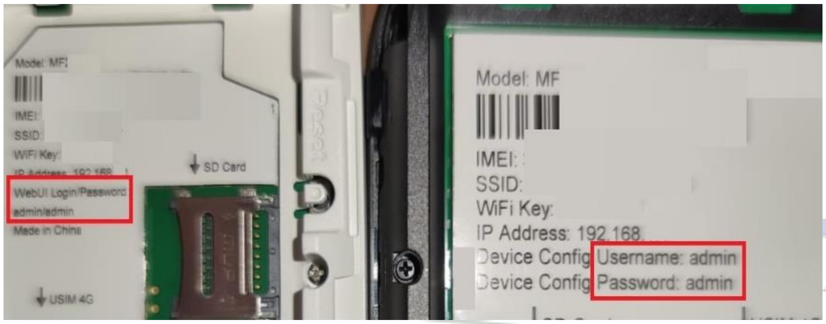
PTA Cyber Security Advisory No.:105 **29-Sep-2020**

Name: Default Credentials Vulnerability

Threat Classification: Gaining Access

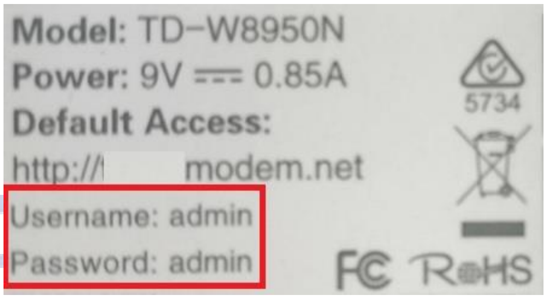
Summary:

Hardware and software products usually come with default credentials (factory settings) which allows user to get full administrative control to perform system configurations. Generally, users do not change default settings / credentials, which may lead to sever security risk.



Model: MF [redacted]
IMEI: [redacted]
SSID: [redacted]
WiFi Key: [redacted]
IP Address: 192.168. [redacted]
WebUI Login/Password
admin/admin
Made in China

Model: MF [redacted]
IMEI: [redacted]
SSID: [redacted]
WiFi Key: [redacted]
IP Address: 192.168. [redacted]
Device Config Username: admin
Device Config Password: admin



Model: TD-W8950N
Power: 9V ⎓ 0.85A
Default Access:
http://[redacted]modem.net
Username: admin
Password: admin

Default credentials of a wide variety of hardware and software products are easily available online and are very easy to guess. Attackers can use them manually or run a script to crawl or scan the internet to look for the exposed or vulnerable devices.

Recommendations:

- It is recommended that Administrators / users should make sure that the default credentials of hardware or software systems have been changed and stored safely before putting in the live environment.
- Devices / Applications manufactured / developed should be designed in way that user must change the default password after 1st use /login.
- Ensure that new passwords used are unique and strong.
- Ensure that unnecessary user accounts have been removed and/or blocked.
- Use alternative Authentication mechanisms like Kerberos, X.509 certificates, public keys, Multi-factor authentication, etc., wherever possible.
- Restrict network access to trusted hosts and networks and allow internet access to the required network services only. If remote access is required, use VPN, SSH, or other secure access methods.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your Security/ Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.