Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:098 **23-July-2020**

Threat Classification: Eavesdropping

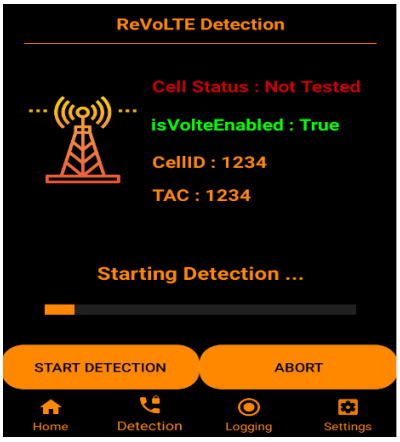
Name: 4G Voice over LTE (VoLTE) Phone Calls Eavesdropping Vulnerability

Affected Systems: Affects the following Telephony service:

- Voice over LTE (VoLTE)

Summary:

It has been reported by the researchers from Ruhr University Bochum, Germany & New York University, Abu Dhabi that a vulnerability in VoLTE protocol can be used to break the encryption on 4G voice calls. This attack is possible because mobile operators often use the same encryption key (called a stream cipher) to secure multiple 4G voice calls that take place via the same base station. The attack has been named as ReVoLTE attack which exploits the reuse of the same keystream for two subsequent calls within one radio connection. This weakness is caused by an implementation flaw of the base station. An Application has also been developed by the researchers that detects whether a base station is vulnerable to the ReVoLTE attack or not.



For further details, please visit following link: https://revolte-attack.net

Recommendations:

- It is strongly recommended to test the aforementioned vulnerability and update the base stations from the vendor provided patches/ fixes.
- It is also recommended to test all the base stations for the aforementioned vulnerability using the App provided by the researchers at:
  https://revolte-attack.net/#app
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, run software with minimal access rights and privileges.
- 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.