Subject:- **Android Vulnerability - Stagefright Bug (Advisory No 11dated Aug 2015)**

Introduction. Recently, a serious vulnerability has been identified in Android operating system which has left most of android phones prone to hacking. The vulnerability is graded very serious as it allows hacking a phone by sending just an MMS which allows stealing of data from mobile.

2. **Method of Infection**. Currently one infection method is known on which a specially crafted MMS / SMS is sent to mobile to compromise it. The exploit is triggered without any user interaction when a media file attached in MMS is received in mobile.

3. **Analysis**

a. **Capability**. Once the files is triggered, it performs following activities:-

(1) Executes remote code.

(2) Makes file untraceable.

(3) Extract images.

(4) Copy and deletes user data.

(5) Takes over microphone and camera.

(6) Tracks user movement through phone GPS.

b. **Method to Identify if Phone is Vulnerable.** Install and use Stage fright Detector App released by Zimperium to check if phone is susceptible to the bug.

c. **Problem in Google Update Mechanism.** Google provides operating system updates directly to nexus phones only.Google also issues the updates to other manufacture like HTC , LG , Motorola, Huawei and Samsung who further issue these updates to users after considerable delays.

4. **Recommendation.** In order to prevent stage fright bug, following is suggested:-

a. Install updates as they are released by phone manufactures..

b. Disable Hangout app and update to latest version before use.

c. **Disable Auto Retrieve of MMS on mobile device.**

d. **Block messages from unknown senders.**

e. Open MMS only from known / trust sources. Even if a known contact sends a file, open it after confirmation.