Subject: **Advisory – Protection against IP Camera Exploitation (Advisory No.2)**

1. **Introduction.** IP cameras are widely used for remote monitoring and surveillance. However, over the period of time various vulnerabilities have been identified in older versions of IP cameras and can be easily exploited for malicious activity. Mostly IP cameras are vulnerable to remote exploitation attacks, especially cameras offered by HIK vision, XVR, Securus, NightOWL, Q-SEE and Cenova.

2. **Technical Analysis.**

a. Common vulnerabilities with available exploits found during analysis of various IP cameras are as following: -

(1) **CVE-2017-11510.** Information leak exists that allows remote attacker to recover the administrator username and password.

(2) **CVE-2017-8224.** Wireless IP Camera have backdoor root account that can be accessed with TELNET.

(3) **CVE-2017-7921.** Improper authentication vulnerability allows escalated privileges and access to sensitive information on system.

(4) **CVE-2017-7923.** Password in configuration file vulnerability allows escalated privileges, access sensitive information and affect integrity.

(5) **CVE-2018-9995.** Allows remote attackers to bypass authentication that provides credentials within JSON data in a response.

b. **Risk Factors.** Following are the major risk factors associated with IP cameras: -

(1) IP cameras often have hard-coded remote-access passwords, hard-coded file-transfer password and a firewall that sometimes malfunctions.

(2) Using one of the affected cameras could greatly endanger a company’s computer network. Attackers can install persistent remote-access malware and can gain unrestricted access to the corporate network and the associated resources.

(3) Remote code execution in IoT network allows attackers to remotely view feeds and tamper with recordings.

3. **Recommendations.**

a. **Never use default camera password,** always make sure that IP camera is protected by strong password which cannot be guessed or brute forced.

b. **Always make sure that OS of IP camera is always kept up-to-date, old version of IP cameras are always vulnerable for attack.**

c. The connections used by IP cameras DVR / NVR / VMS use SSL based encrypted connections.

d. It is recommended that video should be encrypted both when stored on the disk and when it is in transit.

e. IP cameras rely on port forwarding for remote access. Therefore, it is **strongly advised to enable port forward on a few ports and utilize a next generation firewall along with IDS / IPS for further protection.**

f. **Place the security camera system on an air gapped network** or use a separate VLAN.