Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 30) Jun 18**

1. **Introduction.** Critical vulnerabilities have been discovered in **PGP & S/MIME** based encrypted **email clients.** Hackers can easily read encrypted email by exploiting these vulnerabilities.

2. **Technical Details**

   a. PGP and S/MIME are end-to-end encryption standards which are deployed by email server for encryption of email content.

   b. The vulnerability exist in the way an email client handles HTML emails and external resources like loading of images, styles from external URLs.

   c. Email attack issued to break encryption (PGP & S/MIME) anyone having access to email communication can read victim emails in plaintext.

3. **Affected Products.** Following below mentioned plugins / tools used for managing encrypted emails clients are effected by this attack:-

   a. Thunderbird with Enigmail.

   b. Apple Mail with GPGTools.

   c. Outlook with Gpg4win.

4. **Mitigation measures**

   a. Immediately disable above mentioned plugins / tools for emails, clients and apply patches for these vulnerabilities as soon as vendor releases them.

   b. Use authenticated encryption algorithm for sensitive communication.

   c. **Block** AES-GCM at **Authentication encryption (AE)** which is used for attack.,

5. **Recommendations**

   a. Regularly check the vendor website for updates and release of see6rity patches.

   b. Strictly follow all mitigation measures discussed at para 4.

   C. Don't download attachments from emails unless you are sure about the source.

   d. **Install and update ell reputed antiviruses** such as Kaspersky, Avira, Avast etc.

   e. Keep operating system and all softwares up to date.