Subject: **Prevention Against Cyber Espionage - Advisory No 9 March, 2018)**

1. **Introduction.** A critical vulnerability has been found in **"Electron"** a popular web application framework that powers thousands of widely used desktop applications including Skype, Signal, Word press and Slack.

2. **Technical analysis**

a. Electron is an open-source framework that is based on Node.js and Chromium Engine and allows app developers to build cross-platform native desktop applications.

b. Apps can be affected regardless of how the protocol is registered, e.g. using native code, the Windows registry, or Electron's app. set As Default Protocol Client API.

c. Vulnerability details are as under:-

(1)	**CVE Number.**	CVE-2018-1000006.
(2)	**Vulnerability Impact.**	Remote Code Execution.

3. **Affected Product Versions.** The critical vulnerability affects all Microsoft windows based Apps.

4. **Mitigation Measures** Following best practices are suggested in this regard:-

a. The Electron developers have already released two new versions of their framework, i.e. 1.8.2-beta.4, 1.7.11, and 1.6.16 to address this critical vulnerability.

b. Second approach to prevent this attack is to append" -- as the last argument when calling app.setAsDefaultProtocolClient, which prevents Chromium from parsing further options.

c. This vulnerability need to be patched by developers using Electron JS framework as End users can do nothing about this vulnerability.

5. **Secure Coding Practices** Following best coding practices are suggested in this regard:-

a. Only load secure content.

b. Disable the Node.js integration in all renderers that display remote content.

c. Enable context isolation in all renderers that display remote content.

d. Use ses.set Permission Request Handler in all sessions that load remote content.

e. Do not disable web Security.

f. Override and disable eval , which allows strings to be executed as code.

g. Do not set allow Running in secure Content to true.

h. Do not enable experimental.

features. Do not use blink Features.

j. Web Views: Do not use allow popup.

6. Recommendations

a. Regularly check the company website for update's and release of security patch.

b. Strictly follow all mitigation measures discussed at Para 4 and 5.