Subject: **Prevention Against Cyber Espionage Advisory No 08 March 2018**

1. Introduction. Security researchers have found critical vulnerability in "Mozilla Firefox" that could allow remote attackers to execute malicious code on computers running an affected version of the browser.

2. **Technical analysis**

   a. The vulnerability is due to insufficient sanitization of HTML fragments in chrome privileged documents.

   b. To exploit this vulnerability the attacker may use misleading language or instructions to persuade a targeted user to open a crafted file.

   c. Mozilla has confirmed the vulnerability and released software updates.

3. **Affected Product**

   a. Firefox 56 (.0,0.1,0.2).

   b. Firefox 57 (.0,0.1,0.2,0.3,0.4).

   c. Firefox 58(.0).

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

   a. Mozilla has released software update; it is mandatory to update the browser before using it.

   b. Administrators are advised to use an unprivileged account while browsing the internet.

   c. Be careful while using social media groups/ pages and don't click or download any file or image.

   d. Don't open any document received via email or any unknown resource.

   e. Install and update well reputed and licensed antiviruses.

5. **Recommendations**

   a. Regularly check the company website for updates and release of security patch.

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