Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 24) Apr 18**

1. **Introduction.** Recently, a group of serious vulnerabilities have been disclosed by Microsoft that an allow the hackers to remotely take control of the system by just clicking on the malicious link or by just opening website. This vulnerability affects all versions of Windows operating systems to date.

2. **Technical Details.**

   a. An attacker can exploit these issues by tricking the user to open a malicious file or a specially crafted website with the malicious font, which if open in a web browser would hand over control of the affected system to the attacker or it can stop responding to the user.

   b. Microsoft has patched these critical vulnerabilities in Windows Graphics Component that reside in the operating system due to improper handling of embedded fonts by the Windows font library.

   c. These five vulnerabilities found in Windows Microsoft Graphics are listed below:-

      CVE-2018-1010
      CVE-2018-1012
      CVE-2018-1013
      CVE-2018-1015
      CVE-2018-1016

3. **Affected Products.** These vulnerabilities affect the following versions of Microsoft Products:-

   a. Windows 7, 8.1, RT 8.1 and 10.

   b. Windows Server 2008, 2012 and 2016.

4. **Recommendations.**

   a. Install and update well reputed antivirus such as Kaspersky, Bitdefender, Nod 32and Avast etc.

   b. Update all softwares including Windows OS, Microsoft Office and all other softwares. For updating windows to Setting → Update & Security → Windows Update → Check for updates.

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