Subject: **Prevention Against Microsoft Security Flaws (Advisory No 17)**

1. **Introduction.** Various flaws namely CVE-2017-11826, CVE-2017-11779, CVE- 2017-8703 and CVE-2017-11826 have been discovered by security researchers. These flaws reside in various products of Microsoft, which can be exploited by sending a malicious code to an affected product.

2. **Maior Products Affected**

   a. All supported versions of MS Office.

   b. Windows DNS client.

   c. Windows Subsystem for Linux.

   d. Microsoft SharePoint Server.

3. **Impact.** The following flaws once exploited could allow an attacker to perform following activities:-

   a. **CVE-2017-11826.** Attacker could run arbitrary code in the context of the current user i.e. with the same rights as the logged in-user. So, **users with least privilege on their systems are less impacted than those having higher admin rights.**

   b. **CVE-2017-11779.** **Attacker can execute arbitrary code** on Windows clients or Windows Server installations in the context of the software application that made the DNS request.

   c. **CVE-2017-8703.** Attacker can execute a malicious application to affect an object in the memory, which eventually allows that the application **to crash the target system and made it unresponsive.**

   d. **CVE-2017-11826.** Attacker can **perform cross-site scripting (CSS) attacks** on affected systems and execute malicious script in the same

4. **Recommendations.** In order to prevent user's data from being vulnerable to theft, following is suggested:-

   a. Install **October security patches.** Go to Settings > Update & security > Windows Update > Check for updates and install them.

   b. **Backup your files regularly.**

   c. Download email attachments. only from trusted sources. **Even if a known contact sends a file,** open it after confirmation.

   d. Scan system regularly with **antivirus such as Kaspersky, Avira ,Avast, ESET** etc..

   e. Install well **reputed firewall with built-in HIPs** (Host Intrusion Prevention System).