Subject: **Prevention Against Windows 0-Day Flaw (Advisory No,12) Oct 2017**

1. **Introduction.** A zero-day flaw named **Windows .NET Framework RCE(CVE-2017-8759),** was discovered by researchers at cyber security firm FireEye. The zero day allows attacker to take control of complete system. Microsoft NET Framework is available by default in Windows OS which is widely being used in Pakistan. The users are requested to patch their system as highlighted in para 2.

2. **Technologies Affected**

   a. Microsoft .NET Framework 2.0 SP2
   b. Microsoft .NET Framework 3.5
   c. Microsoft .NET Framework 3.5.1
   d. Microsoft .NET Framework 4.5.2
   e. Microsoft .NET Framework 4.6
   f. Microsoft .NET Framework 4.6.1
   g. Microsoft .NET Framework 4.6.2
   h. Microsoft .NET Framework 4.7

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

   a. Take control of an affected system.
   b. Install programs.
   c. View, change, or delete data by tricking victims into, opening a specially crafted document or application sent over an email.
   d. Create new accounts with full user rights.

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

   a. Install security updates regularly as some spywares exploit vulnerabilities.
   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 asIKaspersky, Avira ,Avast, ESET etc.
   e. Install well reputed firewall with built-in Hips (Host Intrusion Prevention System).