SECRET

Subject: **Prevention Against Cyber Espionage (Advisory No 45) Aug 18**

1. **Introduction.** **Cyber Security** researchers have discovered **critical vulnerabilities** in **Microsoft Windows, Microsoft Office, internet explorer (1E), powershell, visual studio** and **adobe flash player .These vulnerabilities** facilitate a **remote attacker** to execute **malicious** code on **vulnerable system.**

2. **Technical Analysis**

   a. **These critical** issues are observed due to **memory corruption flaws** in **internet explorer, edge browser** and **chakra scripting engine.**

   b. **A critical flaw (CVE-2018-8327)** affects Powershell editor services that could allow a **remote attacker** to execute malicious code on **vulnerable system.**

   c. Following the **most critical vulnerabilities** found in **Microsoft Windows** and other softwares:-

      (1) Scripting Engine **Memory Corruption** Vulnerability **(CVE-2018-8242).**

      (2) **Edge Memory** Corruption Vulnerability **(CVE-2018-8262).**

      (3) **Chakra** Memory Corruption Vulnerability **(CVE-2018-8280).**

      (4) Microsoft Edge Memory Corruption Vulnerability **(CVE-2018-8301).**

      (5) Microsoft Edge **Information Disclosure** Vulnerability **(CVE-2018-8324).**

3. **Affected Products.** These vulnerabilities affect **Microsoft Windows** and following softwares:-

   a. Internet Explorer IE
   b. ChakraCore
   c. Microsoft .NET Framework
   d. PowerShell
   e. Visual Studio
   f. Microsoft Office
   g. Adobe Flash Player
   h. Microsoft Share Point
   i. ASP .NET.

4. **Recommendations**

a. **Security patches** have been **released** by all **vendors;** it is strongly advised to **update** against these vulnerabilities.

b. For updating **Microsoft Windows** go to **Setting** → Update & Security → Windows Updates → **Check for updates.**

c. **Install** and **update** well reputed antivirus such as **Kaspersky,** Bitdefender, Nod32 and **Avast** etc.

d. Regularly update all software's including **Windows OS** and **Microsoft Office.**

e. Don't download **attachments** from, unknown emails source.