Subject: - **Cyber Security Advisory - Microsoft Releases Critical Patch Update Including Two Zero-Days (Advisory No. 57)**

Context. Microsoft has patched 49x vulnerabilities including 2x zero-days and 6x critical CVEs in its variety of products e.g. Windows (8,10 and 11), Windows Servers, MS Office, Microsoft Azure, .net framework etc. zero-days include: (CVE-2022-44698) windows smart screen security feature bypass vulnerability and (CVE-2022-44710) graphics kernel privilege escalation vulnerability. Both vulnerabilities allow malicious actors to gain unauthorized control of victims system and perform various privileged operations.

2. **Recommendations**

a. Users and Administrators are requested to examine and apply necessary updates pertaining to specific operating systems and applications offered by Microsoft.

b. Further details on subject vulnerabilities and related patches may be acquired from www.msrc.microsoft.com/update-guide.

c. Regularly monitor endpoints logs for unauthorized activity and access.

d. Harden Windows against exploitation attempts by blocking execution of scripts (.vbe, .vbs, .jse, .js, .bat, .wsf, .hta and .wsh), LOLBins (rundll32.exe, cmd.exe, powershell.exe) and known malicious tools (mimikatz, pwdump, PsExec etc.)