Subject: **Advisory – Prevention against exploitation of Preinstalled Dell Support Assist Utility (Advisory No. 14)**

1. **Introduction**. **Dell Support Assist**, formerly known as Dell System Detect is preinstalled in almost all Dell appliances. Its purpose is to check the health of DELL system's hardware and software for troubleshooting, installation and up-gradation of dell drivers and products. Due to vulnerabilities present in its software, hackers could compromise DELL computers remotely.

2. **Summary of Dell software Vulnerability**

   a. **Vulnerability**. Remote Code Execution

   b. **CVE Identifier**. CVE-2019-3718, CVE-2019-3719

   c. **Severity**. High.

   d. **Affected Product**. Dell Support Assist Client versions prior to 3.2.0.90.

   e. **Vulnerability Information**.

      i. **Improper Origin Validation (CVE-2019-3718)**. A remote attacker could potentially exploit this vulnerability to launch CRSF (Cross site request forgery) attacks on users of the impacted systems.

      ii. **Remote Code Execution Vulnerability (CVE-2019-3719)**. Attacker can compromise the vulnerable system by tricking a victim user into downloading and executing arbitrary executables via Support Assist client from attacker hosted sites.

3. **Recommendations**. **In the light of hazard presented by the presence of remote code execution vulnerability in trusted DELL Support Assist software**, following is recommended:-

   a. **Dell users are recommended to immediately upgrade Dell Support Assist Client version to 3.2.0.90 or latter**.

   b. **Maintain up-to-date antivirus signatures** and engines and keep OS patches up-to-date.

   c. **Disable File and Printer sharing services**. If these services are required, use strong passwords or Active Directory authentication.

   d. **Restrict users' ability (permissions) to install and run unwanted software applications**. Do not add users to the local administrator's group unless required.

   e. **Enable a personal firewall on all workstations and it should be configured to deny unsolicited connection requests**.

f. **Audit your network for systems that use Remote Desktop Protocol (RDP) for remote communication**. Disable the service if not required or install available patches. System administrators may need to work with their technology venders to confirm that patches will not affect system processes.

g. **Make sure that all installed softwares are digitally signed** and validate the authenticity of all downloaded softwares.