Subject:- **Security Flaw in Systems from Dell Inc (Advisory No 16 December 2016)**

Introduction. Dell installed certificate named "eDellRoot" on all new desktop and laptops shipped since August 2015 to make servicing PC issues faster and easier for customers. When a PC connects with Dell Online Support, the certificate provides the system service tag allowing Dell online support to immediately identify the PC model, drivers. OS, hard drive, etc. making it easier and faster to troubleshoot technical issues with customers' computers.

2. **Vulnerability.** The certificate introduced an unintended security vulnerability that exposes users to online eavesdropping and malware attacks. Attackers use the key from Dell to sign phony browser security certificates for any HTTPS-protected site. The malicious hackers exploit the flaw on open, public networks (e.g. WiFi hotspots, coffee shops, airports) to impersonate any Web site to a Dell user, and to quietly intercept, read and modify all of a vulnerable Dell system's Web traffic.

3. **Recommendation**. In order to prevent users, data from being vulnerable to theft, the certificate should be removed from systems by following the instructions attached as Annex A.