Subject:- **Prevention Against Secret Backdoor in Seagate Wireless Hard Drive (Advisory No 14, October 2015)**

Seagate is one of the famous hard disk manufactures. Security researchers of Tangible Security firm revealed multiple vulnerabilities in some Seagate's 3rd generation hard drives that allow hackers to take complete control of the user' s data stored in the hard drive.

2. **Affected Devices**. Following devices having firmware version between 2.2.0.005 and 2.3.0.014 contain respective vulnerability:-

a. Seagate Wireless Plus Mobile Storage.

b. Seagate Wireless Mobile Storage - wirelessly streaming tablet and Smartphone's data.

c. LaCie FUEL- wirelessly extending storage for iPads.

3. **Method of Operation**. Following are known methods of infection that enable hackers to extract:-

a. While the drive is connected to network, undocumented Telnet service of hard drive can be accessed or by using the default credentials of 'root' as username and and password - CVE-2015-2874 vulnerability.

b. Unrestricted file downloading under default configuration of the hard drive-CVE-2015-2875 vulnerability.

c. File uploading to the device's /media/sda2 file system. under default configuration - CVE-2015-2876 vulnerability.

4. **Recommendation**. In order to prevent user's data from being vulnerable to theft, users have to update the device firmware to version 3.4.1.105 or latest.