Subject: **Advisory on Vulnerability in Encryption Protocol (Advisory No. 07 dated 8th April, 2016)**

1. **Introduction.** Internet communication is increasingly becoming encrypted which has made it safe against eavesdropping. However such encryption techniques are prone to hacking due to vulnerabilities that may lead to leakage of information while surfing the web.

2. DROWN attack is a vulnerability that affects HTTPS protocols that allows eavesdropping on some encrypted communication.

3. **Technical Details (For System Administrators).** DROWN attack stands for "Decrypting RSA with Obsolete and Weakened eNcryption". It is a vulnerability that affects HTTPS protocol and other services that rely on SSL and TLS. Due to mis configurations, many servers still are using SSLv2 which is an old protocol. It allows an attacker to decrypt modern TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

4. **Affected Servers.** Following servers are vulnerable to DROWN Attack:-

- **a.** If it allows SSLv2 connections.
- **b.** If its private key is used on any other server that allows SSLv2 connections.

5. **Recommendations.** Systems administrators are advised to carry out following measures:-

- **a.** OpenSSL 1.0.2 be upgraded to 1.0.2g.
- **b.** OpenSSL 1.0.1 be upgraded to 1.0.1s.
- **c.** Ensure that the **SSLv2** '**is disabled** in all SSL/TLS servers (VPN, VolP, Email, Web servers etc)
- **d.** Ensure that private key isn't shared across any other servers that support SSLv2 communication.