Advisory Detail

Date: ***01/03/2016***

Alert Level: ***HIGH***

Advisory Name: ***OpenSSL Security Advisory [DROWN]***

Summary:

DROWN is a vulnerability that affects HTTPS, and associated services like browsing the internet, mail, Instant messages that rely on SSL/TLS.

DROWN allows attackers to decrypt the communication and steal sensitive information like passwords, financial data, emails, Instant messages, and credit card numbers.

Description:

Cross-protocol attack on TLS using SSLv2 (**DROWN**) (CVE-2016-0800) **DROWN** is stands for **Decrypting RSA with Obsolete and Weakened eNcryption**. **DROWN** is made worse by two additional OpenSSL implementation vulnerabilities. CVE-2016-0703 and CVE-2015-3197.

Impact:

This attack could result a decryption of TLS session between SSLv2 server and EXPORT cipher suites.

System Affected:

This issue affects OpenSSL versions 1.0.2 and 1.0.1

Q-CERT Recommendation :

- Risk could be avoided by disabling the SSLv2 protocol in all their SSL/TLS servers.

- Risk could be mitigated by :
  - Apply upgrade OpenSSL 1.0.2 to OpenSSL 1.0.2g
  - Apply upgrade OpenSSL 1.0.1 to OpenSSL 1.0.1s

- Report any Incident related to OpenSSL Vulnerability to Q-CERT Team via the following:
  - Website: www.qcert.org
  - Hotline: +974 – 44933408
  - Incidents Mailbox: incidents@qcert.org

References :

- OpenSSL Security Advisory [1st March 2016] : https://www.openssl.org/news/secadv/20160301.txt

- DROWN Technical White-Paper : https://drownattack.com/drown-attack-paper.pdf

- Check if your Website is vulnerable : https://drownattack.com/#check

- DROWN Vulnerability Q&A : https://drownattack.com/#question-answer