Alert Details

Date: 9 April *2014*

Alert Level: ***High***

Alert Name: *OpenSSL Vulnerability "Bleeding Heart"*

Systems Affected:

- OpenSSL 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

Overview:

Security researchers disclosed a vulnerability in **OpenSSL** that could allow a remote attacker to expose sensitive data, including user authentication credentials and secret keys.

Impact:

OpenSSL is widely used in popular applications and systems like BIND, OpenSSH, Various Linux Distributions, Apache servers, Various Java Applications, VPNs, Mobile devices Authentication, Open source browsers…etc. Furthermore, Q-CERT labeled this threat as high due to the following:

- Publically available exploit code
- Attack leaves no traces on the server logs
- Sensitive data sent over TLS/SSL such as login information, passwords, credit card numbers, etc.

Vulnerability Description:

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in its implementation of the TLS/DTLS heartbeat functionality "Hence the Bleeding Heart" name. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable **OpenSSL** library in "unlimited" chunks of 64k, one at a time. The sensitive information that can be exposed using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

Q-CERT Recommendation:

1. Inventory all systems and servers running the affected versions of OpenSSL
2. Upgrade to the latest version **OpenSSL 1.0.1g** from http://www.openssl.org/news/secadv_20140407.txt
3. Revoke compromised keys and reissue new keys from the Certificate Authority
4. Change user passwords and encryption keys
5. All old session keys and session cookies must be revoked, expired/invalidated.
6. Work with vendors as more are publishing patches that fix this problem, vendors such as Red Hat, CentOS, Ubuntu already fixed their repositories.

Note: Any encryption keys generated with one of the affected **OpenSSL** versions should be considered compromised and should not be trusted.

For more information:

- http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html
- http://www.kb.cert.org/vuls/id/720951
- http://heartbleed.com/

Organizations are advised to contact Q-CERT immediately in case they experience any suspicious activity on the following email address incidents@qcert.org