NOTA MAKLUMAN GCERT BIL. 1/2014
PADA 9 APRIL 2014

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**OpenSSL Heartbleed Information Disclosure Vulnerability**
Tarikh Dikesan	**9 April 2014**
Bilangan Agensi Terlibat	**Semua**

Sistem Pengoperasian/Aplikasi Berisiko

- OpenSSL Versions 1.0.1 - 1.0.1f

Kaedah Serangan

- Penceroboh membaca memori sistem dan mengambil maklumat berkaitan kata kunci rahsia yang digunakan untuk mengenal pasti pembekal perkhidmatan bagi menyulit (*encrypt*) trafik, nama pengguna, kata laluan dan kandungan.

Kesan Serangan

- Kesan daripada kelemahan ini adalah penceroboh boleh mendapat maklumat yang sensitif seperti kata kunci rahsia (*private key*). Dengan menggunakan maklumat sensitif tersebut, penceroboh boleh membuat *decrypt*, *spoof* dan melaksanakan serangan *man-in-the-middle* ke atas trafik rangkaian.

Cadangan Tindakan Pengukuhan

- Menaiktaraf OpenSSL ke versi terkini.
- "Disable" fungsi OpenSSL Heartbleed Support

Maklumat Lanjut

- http://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/963/index.html