NOTA MAKLUMAN SGCERT BIL. 1/2015
PADA 9 MAC, 2015

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**: FREAK SSL/TLS**
Tarikh Dikesan	**: 3hb Mac, 2015**
Bilangan Agensi Terlibat	**: Semua Pengguna Rangkaian Sabah.Net**

Sistem Pengoperasian/Aplikasi Berisiko

- Semua jenis *servers*
- Semua jenis *browsers* termasuk *browser* yang digunakan dalam telefon pintar (smartphones)

Kaedah Serangan

- Keterdedahan dalam *OpenSSL* (cth. Android), *Apple SecureTransport* (cth. Safari), *Microsoft Schannel TLS Library* dan *Apache mod_ssl*
- Keterdedahan ini membolehkan pencoroboh memintas perhubungan HTTPS diantara browsers dan servers dan memaksa menggunakan enkripsi yang lemah dan mudah dipantau.
- Keadah serangan ini dikenali sebagai 'man-in-the-middle attack'.

Kesan Serangan

- Seseorang pencoroboh itu dapat mencuri maklumat data yang sensitif dalam talian diantara *browser* dan *server* yang dilawati dan seterusnya menyalahgukakan data tersebut.

Cadangan Tindakan Pengukuhan

Server:

- Uji kekukuhan *server* jika terdedah kepada FREAK dengan menggunakan *tool* di laman:
  - SSL FREAK Check: *https://tools.keycdn.com/freak*
  - SSL Server Test: *https://www.ssllabs.com/ssltest/*
- Rujuk https://technet.microsoft.com/en-US/library/security/MS15-031
- Pastikan *OpenSSL* adalah versi 1.0.1k keatas
  - Rujuk https://www.openssl.org/news/secadv_20150108.txt

Browser (Clients):

- Uji samada *browser* anda selamat digunakan dengan melayari ke laman
  - https://freakattack.com/clienttest.html
- Kemaskini semua *browser* yang selalu digunakan.

Maklumat Lanjut

- *https://freakattack.com/*
- https://www.smacktls.com/
- https://technet.microsoft.com/en-US/library/security/MS15-031
- https://www.openssl.org/news/secadv_20150108.txt

Disediakan oleh:
Research and Development Team, sgCERT
Urusetia sgCERT
Bahagian Keselamatan
Jabatan Perkhidmatan Komputer Negeri