NOTA MAKLUMAN GCERT BIL. 3/2012
PADA 17 OKTOBER 2012

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**RSA Weak Certificate Vulnerability**
Tarikh Dikesan	**17 Oktober 2012**
Bilangan Agensi Terlibat	**Semua agensi yang menggunakan Ms Windows dengan panjang kekunci sijil RSA kurang dari 1024 bit**

Sistem Pengoperasian/Aplikasi Berisiko

* Ms Windows XP (32-bit & 64-bit)
* Ms Windows Vista (32-bit & 64-bit)
* Ms Windows 7 (32-bit & 64-bit)
* Ms Windows Server 2003 (32-bit, 64-bit & IA-64 bit)
* Ms Windows Server 2008 (32-bit, 64-bit & IA-64 bit)
* Ms Windows Server 2008 R2 (64-bit & IA-64 bit)
* Ms Windows Embedded Standard 7 (32-bit & 64-bit)

Kaedah Serangan

Penceroboh akan menghasilkan sijil RSA palsu dengan panjang kekunci kurang dari 1024 bit dan menggunakan sijil tersebut untuk menyamar sebagai pengguna yang sah.

Kesan Serangan

i. Penceroboh dapat mengakses dan mengubah maklumat terperingkat Kerajaan; dan
ii. Pihak agensi akan terdedah kepada pelbagai ancaman keselamatan ICT memandangkan semua security patch daripada pihak Microsoft memerlukan panjang kekunci sijil RSA sekurang-kurangnya 1024 bit.

Cadangan Tindakan Pengukuhan

i. Memastikan semua sijil RSA yang digunakan mempunyai panjang kekunci sekurang-kurangnya 1024 bit;
ii. Memasang KB2749655 *update* menggunakan Microsoft Update; dan
iii. Membuat pengujian bagi memastikan semua aplikasi berfungsi dengan baik setelah pemasangan KB2749655 (pemasangan KB2749655 mungkin akan mengganggu aplikasi lain yang menggunakan panjang kekunci sijil RSA kurang dari 1024 bit).

Maklumat Lanjut

1. http://technet.microsoft.com/en-us/security/advisory/2749655
2. http://support.microsoft.com/kb/2661254