NOTA MAKLUMAN GCERT BIL. 3/2013
PADA 11 APRIL 2013

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**Joomla JCE 2.0.10 Shell Upload Exploit**
Tarikh Dikesan	**9 April 2013**
Bilangan Agensi Terlibat	**Semua**

Sistem Pengoperasian/Aplikasi Berisiko

- Joomla CMS versi 1.5 (dan ke atas) yang menggunakan komponen JCE versi 2.0.10

Kaedah Serangan

- Penceroboh akan mengeksploit kelemahan ImageManager pada komponen JCE dengan memuatnaik fail berbahaya/*backdoor* dalam bentuk fail grafik dan seterusnya menukar nama fail tersebut ke fail PHP.

Kesan Serangan

- Penceroboh akan mempunyai kawalan sepenuhnya ke atas server agensi;
- Penceroboh berupaya untuk mengubah/memadam maklumat yang terdapat pada server; dan
- Server agensi mungkin akan digunakan untuk menyerang lain-lain server.

Cadangan Tindakan Pengukuhan

- Menaiktaraf komponen Joomla JCE ke versi terkini; dan
- Mengemaskini konfigurasi fail ‘htaccess’ bagi menghalang lain-lain serangan ke atas Joomla CMS.

Maklumat Lanjut

- http://www.joomlacontenteditor.net/news/item/jce-and-your-sites-security
- http://ustechnica.com/2013/01/09/joomla-vulnerability/
- http://www.bowlerhat.co.uk/archive/adding-additional-rewrite-rules-to-joomla-htaccess/