NOTA MAKLUMAN GCERT BIL. 2/2012
PADA 7 OGOS 2012

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**XMLRPC Vulnerability**
Tarikh Dikesan	**6 Ogos 2012**
Bilangan Agensi Terlibat	**Semua agensi yang mempunyai fail 'xmlrpc.php' pada server web/portal**

Sistem Pengoperasian/Aplikasi Berisiko

* Semua aplikasi web yang mempunyai fail 'xmlrpc.php'

Kaedah Serangan

Penceroboh akan mengeksploit fungsi kemaskini fail yang terdapat di dalam fail 'xmlrpc.php' dan digunakan untuk memuatnaik fail *backdoor/malware* ke server web agensi.

Kesan Serangan

Penceroboh dapat mengawal server agensi secara jarak jauh melalui fail *backdoor/malware* yang telah dimuat naik.

Cadangan Tindakan Pengukuhan

i. Menaiktaraf PEAR XML_RPC ke versi terkini;
ii. Memadamkan fail 'xmlrpc.php' (jika tidak diperlukan);
iii. Menaiktaraf aplikasi laman web/portal (Joomla, WordPress, dll.) ke versi terkini; dan
iv. Menghadkan fungsi PHP yang merbahaya (php.ini), cth:

```
disable_functions =
exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini
```

Maklumat Lanjut

1. http://www.hardened-php.net/advisory_142005.66.html
2. http://www.securityfocus.com/bid/45299
3. http://xforce.iss.net/xforce/xfdb/33470