26/02/2010 - Wordpress 2.9.2 in pericolo!

Già da ieri il mio amico clshack aveva pubblicato un articolo tramite il quale ci informava che la sua installazione di wp 2.9.2 era stata attaccata da uno spiderbot che tramite una falla dell'ultima versione di wp (ancora non si sà molto in merito) era riuscito ad inniettare del codice all'interno del file wp-config.php che provocava il redirect del visitatore verso un altro sito.
Oggi tramite un nuovo articolo che potete trovare qui fa luce sul meccanismo utilizzato durante l'attacco e per nostra fortuna ci suggerisce un workaround per impedire che anche il nostro sito venga bucato tramite questo espediente. Ripropongo lo snippet di codice qui per comodità ma vi suggerisco di leggere l'articolo di clshack che è molto più esaustivo.

Ci basta inserire questo controllo all'inizio del nostro header file... naturalmente del template che stiamo utilizzando:

```
<?phpArrayif (strlen($_SERVER['REQUEST_URI']) > 155
||Array strpos($_SERVER['REQUEST_URI'], "eval")
||Array strpos($_SERVER['REQUEST_URI'], "base64")) {Array  @header("HTTP/1.1 414
Request-URI Too Long");Array  @header("Status: 414 Request-URI Too
Long");Array  @header("Connection: Close");Array  @exit;Array} ?>
```

Se analizziamo brevemente lo snippet possiamo notare che blocca tutte le richieste al server maggiori di 155 caratteri e che contengono all'interno le stringhe "eval" e "base64? poichè è proprio tramite queste richieste che viene portato avanti l'attacco.

A rigor di logica questo è solo una pezza da utilizzare prima di una NECESSARIA patch ufficiale!

Be Sociable, Share!

-
-
-
-
-
-

■

- Tweet
-
-
-
-