

PHP-based CMS mass-exploitation

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-03/msg00134.html>

- *From:* "Daniel Bonekeeper" <thehazard@xxxxxxxxxx>
 - *Date:* Tue, 7 Mar 2006 10:56:46 -0500
-

This is not the first time that we see those kind of "attacks", but on the recent days, I've noticed those requests on my webservers with a considerable frequency:

```
83.84.14X.XXX -- [06/Mar/2006:18:18:12 -0500] "GET
/index2.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:13 -0500] "GET
/index.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1
HTTP/1.1" 200 10110 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:14 -0500] "GET
/mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:15 -0500] "GET
/cvs/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:17 -0500] "GET
/articles/mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:18 -0500] "GET
/cvs/mambo/index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:19 -0500] "POST /xmlrpc.php
HTTP/1.1" 200 375 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:20 -0500] "POST /blog/xmlrpc.php
HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:21 -0500] "POST
/blog/xmlsrv/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:22 -0500] "POST
/blogs/xmlsrv/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0
```

PHP-based CMS mass-exploitation

```
(compatible; MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:23 -0500] "POST
/drupal/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:25 -0500] "POST
/phpgroupware/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:26 -0500] "POST
/wordpress/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:27 -0500] "POST /xmlrpc.php
HTTP/1.1" 200 375 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:28 -0500] "POST
/xmlrpc/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1;)"
83.84.14X.XXX -- [06/Mar/2006:18:18:29 -0500] "POST
/xmlsrv/xmlrpc.php HTTP/1.1" 404 8696 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1;)"
```

All of them, as we can see, are exploitation attempts to known bugged pages (like the newest Mambo bug, the old XMLRPC problem with old versions of Drupal, etc). I guess that they are getting a list of domain names and trying them out with those vulns, and I believe that they may already have some thousands of vuln machines in their hands. Such attacks might be enhanced by using Google to guess which domains are using which CMS... for example, looking on Google for "A password and instructions will be sent to this e-mail address, so make sure it is accurate." will return a bunch of Drupal websites (88,500 according to Google, even though we can see just the first 1000 ones).

This is just an advise for all admins that use those CMS, to keep, as always, your CMS updated (almost every two weeks there are new vulns disclosed), and also, check if you already got caught by that, if you're running old software.

--

```
# (perl -e "while (1) { print "\x90"; }") | dd of=/dev/evil
```