

[Full-disclosure] mambo remote code sexecution

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-11/0535.html>

From: peter MC tachatte (*slythers_at_gmail.com*)

Date: 11/16/05

Date: Wed, 16 Nov 2005 16:44:28 +0100
To: full-disclosure@lists.grok.org.uk

a vulnerability exist in globals.php when register_globals is off and allow remote code inclusion

this a GLOBALS overwrite
in components/com_content/content.html.php
there is the line:
require_once(\$GLOBALS['mosConfig_absolute_path'] .
'/includes/HTML_toolbar.php');

ok

da globals.php:

```
if (!ini_get('register_globals')) {  
while(list($key,$value)=each($_FILES)) $GLOBALS[$key]=$value;  
while(list($key,$value)=each($_ENV)) $GLOBALS[$key]=$value;  
while(list($key,$value)=each($_GET)) $GLOBALS[$key]=$value;  
while(list($key,$value)=each($_POST)) $GLOBALS[$key]=$value;  
while(list($key,$value)=each($_COOKIE)) $GLOBALS[$key]=$value;  
while(list($key,$value)=each($_SERVER)) $GLOBALS[$key]=$value;  
while(list($key,$value)=@each($_SESSION)) $GLOBALS[$key]=$value;  
foreach($_FILES as $key => $value){  
$GLOBALS[$key]=$_FILES[$key]['tmp_name'];  
foreach($value as $ext => $value2){  
$key2 = $key . '_' . $ext;  
$GLOBALS[$key2] = $value2;  
}  
}  
}
```

da fake protect in mambo.php:

```
if (in_array( 'globals', array_keys( array_change_key_case( $_REQUEST,  
CASE_LOWER ) ) ) ) {  
die( 'Fatal error. Global variable hack attempted.' );  
}  
if (in_array( '_post', array_keys( array_change_key_case( $_REQUEST,  
CASE_LOWER ) ) ) ) {
```

Full-Disclosure: [Full-disclosure] mambo remote code sexecution

```
die( 'Fatal error. Post variable hack attempted.' );  
}  
poc: http://enviede.wistee-heb.fr/index.php?cat=poc  
slythers@gmail.com
```

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>