

Mambo OS v4.5/v4.6: remote command execution

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-01/0139.html>

From: FraMe (frame_at_hispalab.com)

Date: 01/18/04

To: <bugtraq@securityfocus.com>

Date: Sun, 18 Jan 2004 18:21:15 +0100

Product: Mambo Open Source v4.5

Mambo Open Source v4.6 (CVS)

Vendor: Miro International Pty Ltd.

Author: FraMe ([frame at kernelpanik.org](mailto:frame@kernelpanik.org))

URL: <http://www.kernelpanik.org>

CONTENTS

1. Overview
2. Description.
3. Details
4. Patches.

1. Overview.

Mambo Open Source is an, open source, modular, web content management system (CMS), written in Php with a MySql database in backend.

More info: <http://www.mamboserver.com>

2. Description.

Mambo OS allow remote command execution in `./modules/mod_mainmenu.php`
Anybody can inject a url in `$mosConfig_absolute_path` and obtain command execution
with web server privileges (usually nobody).

3. Details.

Mambo OS v4.5 and v4.6

from `./modules/mod_mainmenu.php`:

=====

```
<?php
```

```
(..)
```

SecurityFocus Bugtraq: Mambo OS v4.5/v4.6: remote command execution

```
// $module is defined in the calling function
```

```
// $params is defined in the calling function
```

```
require_once( "$mosConfig_absolute_path/modules/mod_mainmenu.class.php" );
```

```
(..)
```

```
?>
```

4. Patches

a) Php globals off (Default in Php > 4.2)

b) Unofficial patch for mod_mainmenu.php can be downloaded from:

<http://www.kernelpanik.org/code/kernelpanik/mambo.zip>

```
=====
```

[FraMe – frame at kernelpanik.org]

[URL – <http://frame.lifefromthenet.com>]

[Kernelpanik – <http://www.kernelpanik.org>]

[PGP KeyID – 0xFA81AC9C]

```
=====
```